

University of Warwick institutional repository: <http://go.warwick.ac.uk/wrap>

**A Thesis Submitted for the Degree of PhD at the University of Warwick**

<http://go.warwick.ac.uk/wrap/57023>

This thesis is made available online and is protected by original copyright.

Please scroll down to view the document itself.

Please refer to the repository record for this item for information to help you to cite it. Our policy information is available from the repository home page.

# Unipotent Subgroups of Reductive Algebraic Groups

RICHARD PROUD

Thesis submitted for the degree of Doctor of Philosophy  
Mathematics Institute, University of Warwick  
September 1997

# Contents

Acknowledgements and Declaration . . . . .	iii
Summary . . . . .	iv
Frequently Used Notation . . . . .	v
Dynkin Diagrams . . . . .	vi
<b>0 Introduction</b>	<b>1</b>
<b>1 Witt Groups and Artin-Hasse Exponentials</b>	<b>4</b>
1.1 Witt Vectors . . . . .	6
1.2 Witt Groups and Connected Abelian Unipotent Groups . . . . .	16
1.3 The Functional Equation Lemma . . . . .	23
1.4 Applications . . . . .	30
1.5 Witt Groups and Artin-Hasse Exponentials . . . . .	36
1.6 Artin-Hasse Exponentials of Nilpotent Matrices . . . . .	40
1.7 Complex Artin-Hasse Exponentials . . . . .	47

<b>2</b>	<b>Simple Algebraic Groups</b>	<b>49</b>
2.1	Regular Unipotent Elements . . . . .	50
2.2	Type $A_l$ . . . . .	53
2.3	Type $C_l$ . . . . .	59
2.4	Type $B_l$ . . . . .	67
2.5	Type $D_l$ . . . . .	73
2.6	Type $G_2$ . . . . .	80
2.7	Type $F_4$ . . . . .	91
2.8	Type $E_n$ , $n = 6, 7, 8$ . . . . .	104
2.9	The Adjoint Case . . . . .	111
<b>3</b>	<b>Reductive Algebraic Groups</b>	<b>113</b>
3.1	The Cayley Transform . . . . .	114
3.2	Semiregular Unipotent Elements . . . . .	121
3.3	The Main Theorem . . . . .	123
3.4	Appendix A . . . . .	126
3.5	Appendix B . . . . .	128
3.6	Appendix C . . . . .	133
	<b>Bibliography</b>	<b>135</b>

# Acknowledgements

Firstly, I would like to thank my supervisor, Dr. D.M. Testerman, for originally suggesting this problem, and for her continued support and encouragement during the preparation of this thesis.

I would also like to thank Prof. R.W. Carter for his kind assistance and guidance throughout my studies at Warwick.

Also thanks to Dr. R. Lawther for many useful and interesting conversations, and to Ben Carr for his assistance with the Magma computer programs used in 2.8.

I am especially grateful to my parents and family for their support, both on a personal and financial level.

Finally, I would like to thank the Engineering and Physical Sciences Research Council, and the Mathematics Institute, for providing my funding.

## Declaration

The results in this thesis are, to the best of my knowledge, original except where otherwise stated.

# Summary

Let  $G$  be a connected reductive algebraic group defined over an algebraically closed field of *good* characteristic  $p > 0$ . Suppose  $u \in G$  has order  $p$ . In [T2] it is shown that  $u$  lies in a closed reductive subgroup of  $G$  of type  $A_1$ . This is the best possible group theoretic analogue of the Jacobson-Morozov theorem for simple Lie algebras. Testerman's key result is a type of 'exponentiation process'. For our given element  $u$ , this process constructs a 1-dimensional connected abelian unipotent subgroup of  $G$ , hence isomorphic to  $\mathbb{G}_a$ , containing  $u$ . This in turn yields the required  $A_1$  overgroup of  $u$ .

Now let  $1 \neq u \in G$  be an arbitrary unipotent element. Such an element has order  $p^t$ , for some  $t \in \mathbb{N}$ . In this thesis we extend the above result, and show that  $u$  lies in a  $t$ -dimensional closed connected abelian unipotent subgroup of  $G$ , provided  $p > 29$  when  $G'$  contains a simple component of type  $E_8$ , and that  $p$  is good for the remaining components. The structure of the resulting unipotent overgroup is also explicitly given. This is the best possible result, in terms of 'minimal dimension', which we could hope for.

In Chapter 1 we discuss the theory of Witt vectors, associated with a commutative ring with identity. They are closely related to the study of connected abelian unipotent algebraic groups. The unipotent overgroups are constructed using a variation of the usual exponentiation process. The necessary material on formal power series rings is given in 1.3. The Artin-Hasse exponentials of 1.4 play a crucial role in this construction. The connection between Witt groups and Artin-Hasse exponentials is discussed in 1.5.

In Chapter 2 we apply the techniques of Chapter 1 to the various simple algebraic groups. For each type, a particular isogeny class is chosen and the required overgroup is constructed for the regular (and subregular) classes. In 2.9 we pass to the adjoint case.

In Chapter 3 we extend the results of Chapter 2 to include all unipotent classes in all reductive algebraic groups (under certain restrictions). In 3.1 the Cayley Transform for the classical groups is combined with the ideas of Chapter 1 to give an explicit construction of the unipotent overgroups for every unipotent class. In 3.2 we discuss semiregular unipotent elements. Finally, in 3.3, we prove the main theorem of this thesis.

# Frequently Used Notation

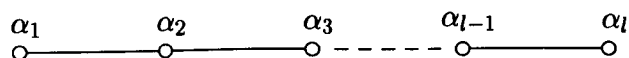
We use  $\mathbb{N}$ ,  $\mathbb{Z}$ ,  $\mathbb{Q}$ , and  $\mathbb{C}$  to denote (respectively) the natural numbers, the integers, the rational numbers, and the complex numbers. Let  $n \in \mathbb{N}$ . Write  $(x, y)$  for the greatest common divisor of  $x, y \in \mathbb{Z}$ , not both zero.

<u>Symbol</u>	<u>Meaning</u>	<u>Page introduced</u>
$\dim(G)$	dimension of $G$	3
$e_{ij}$	elementary matrix with 1 in $(i, j)$ -th position	42
$G$	(algebraic) group	1
$G^\circ$	identity component of $G$	3
$G_u = \mathcal{U}$	unipotent variety of $G$	1
$G' = (G, G)$	commutator subgroup of $G$	2
$\mathbb{G}_a, \mathbb{G}_m$	additive group of $K$ , multiplicative group of $K$	1, 21
$GL(n, R)$	general linear group of degree $n$ over $R$	1
$\overline{H}$	closure of subgroup $H$ of $G$	3
$K$	algebraically closed field	1
$K^n$	$n$ -tuples over $K$	4
$M(n, R)$	$n \times n$ matrices over $R$	40
$o(x)$	(finite) order of $x \in G$	1
$p\text{-nilp}(N)$	$p$ -nilpotency of nilpotent $0 \neq N \in M(n, R)$	40
$R$	commutative ring with identity	9
$R[X]$	polynomial ring in indeterminate(s) $X$ over $R$	6
$R[X]_0$	elements of $R[X]$ with zero constant term	35
$R[[T]]$	formal power series ring in indeterminate $T$ over $R$	23
$R[[T]]_0$	elements of $R[[T]]$ with zero constant term	23
$SL(n, R)$	special linear group of degree $n$ over $R$	42
$U$	maximal connected unipotent subgroup of $G$	50
$U(n, R)$	$n \times n$ uni-upper triangular matrices over $R$	42
$u(n, R)$	$n \times n$ strictly upper triangular matrices over $R$	42
$W(R)$	Witt ring over $R$	7, 13
$W_n(R)$	$n$ -th Witt ring over $R$	5, 13
$\mathbb{Z}_{(p)}$	$\{x/y : x \in \mathbb{Z}, y \in \mathbb{Z} - 0, (y, p) = 1\}$ , $p \in \mathbb{N}$ prime	30
$Z = Z(G)$	centre of $G$	51
$Z_G(x)$	centralizer of $x \in G$	50

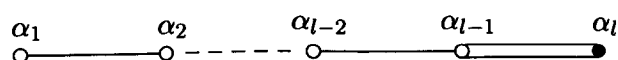
# Dynkin Diagrams

We give below the Dynkin diagrams of the various irreducible root systems. The darkened nodes represent the short roots.

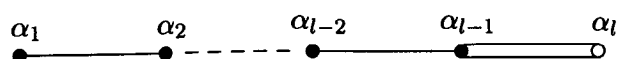
Type  $A_l$  ( $l \geq 1$ ) :



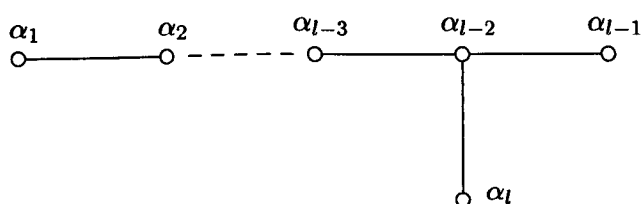
Type  $B_l$  ( $l \geq 2$ ) :



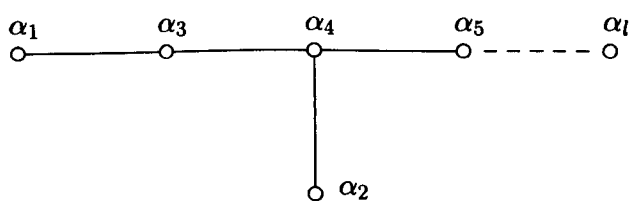
Type  $C_l$  ( $l \geq 3$ ) :



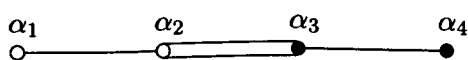
Type  $D_l$  ( $l \geq 4$ ) :



Type  $E_l$  ( $l = 6, 7, 8$ ) :



Type  $F_4$  :



Type  $G_2$  :





# Chapter 0

## Introduction

Let  $G$  be a reductive algebraic group defined over an algebraically closed field  $K$  of characteristic  $p \geq 0$ . We will always assume that such a group is connected. Suppose  $1 \neq u \in G_u$  is a unipotent element. If  $p = 0$  then  $u$  has *infinite* order, since any element with finite order must be diagonalizable; that is, semisimple. Now suppose  $p > 0$ . For the group  $GL(n, K)$ ,  $n \in \mathbb{N}$ , we have the following:

$$v \text{ is unipotent} \quad \Leftrightarrow \quad v^{p^t} = I_n \text{ for some } t \geq 0.$$

Indeed write  $v = I_n + N$ , where  $N$  is a nilpotent  $n \times n$  matrix, then  $v^{p^t} = (I_n + N)^{p^t} = I_n + N^{p^t}$ , with  $N^{p^t} = 0$  for large enough  $t$ . The converse argument works in a similar way. Regarding  $G$  as a closed subgroup of  $GL(n, K)$ , for some  $n \in \mathbb{N}$ , it follows that

$$1 \neq u \in G \text{ is unipotent} \quad \Leftrightarrow \quad o(u) = p^t \text{ for some } t \in \mathbb{N}.$$

In particular, the unipotent elements have *finite* order. Note that if  $s \in G$  has finite order *coprime* to  $p$ , then it is semisimple as above.

In [T2], the following natural question was addressed: Given a unipotent element  $1 \neq u \in G_u$ , under what conditions does there exist a closed reductive subgroup  $H$  of  $G$ , of type  $A_1$ , with  $u \in H$ ? When  $p = 0$  there are no restrictions. Now suppose  $p > 0$ . The maximal connected unipotent subgroups of a group  $H$  of type  $A_1$  are all 1-dimensional, and so are isomorphic to  $\mathbb{G}_a$ . Therefore any non-identity unipotent element of  $H$  must have order  $p$ .

Testerman shows that this is a sufficient condition, at least when  $p$  is a *good* prime for  $G$ : The good primes for the various *simple* algebraic groups are given below.

Type	$A_l$	$B_l, C_l, D_l$	$G_2, F_4, E_6, E_7$	$E_8$
Good primes	all $p$	$p > 2$	$p > 3$	$p > 5$

In turn  $p$  is good for  $G$  if it is good for each simple component of  $G'$ . Otherwise  $p$  is *bad* for  $G$ . We have the following

**Theorem** ([T2,4.1]) *Let  $G$  be a reductive algebraic group defined over an algebraically closed field  $K$  of good characteristic  $p > 0$ . Let  $1 \neq u \in G_u$  be unipotent, with  $\text{o}(u) = p$ . Then there exists a closed reductive subgroup  $H$  of  $G$ , of type  $A_1$ , with  $u \in H$ .*

This result is the group theoretic analogue of the Jacobson-Morozov Theorem for simple Lie algebras (see [J2]). The following is an immediate consequence of the above results:

**Corollary** *Let  $G$  be a reductive algebraic group defined over an algebraically closed field  $K$  of characteristic  $p$ , where either  $p = 0$ , or  $p > 0$  is a good prime for  $G$ . Let  $1 \neq u \in G_u$  be unipotent. If  $p > 0$ , impose the restriction  $\text{o}(u) = p$ . Then  $u$  lies in a 1-dimensional closed connected abelian unipotent subgroup  $V$  of  $G$ , with  $V \cong \mathbb{G}_a$ .*

The above corollary in the case  $p = 0$  can be obtained in a more elementary way as follows: View  $G$  as a closed subgroup of  $GL(n, K)$  for some  $n \in \mathbb{N}$ , and suppose  $I_n \neq u \in G_u$  is a unipotent matrix. Then  $u = I_n + N$ , where  $0 \neq N$  is a nilpotent  $n \times n$  matrix. Suppose  $N^e = 0$  with  $N^i \neq 0$ ,  $1 \leq i < e$ , and define

$$\exp(N) = \sum_{i=0}^{e-1} \frac{N^i}{i!} \quad \text{and} \quad \log(u) = \sum_{i=1}^{e-1} \frac{(-1)^{i+1}}{i} N^i,$$

where  $N^0 = I_n$ . Clearly,  $\exp(N)$  is a unipotent matrix in  $GL(n, K)$ , and  $\log(u)$  is a nilpotent  $n \times n$  matrix. Moreover we have

$$\exp(\log u) = u \quad \text{and} \quad \log(\exp N) = N,$$

which follow from [B1,IV,4.10]. Consider the following map

$$\begin{aligned} \phi : \mathbb{G}_a &\rightarrow GL(n, K) \\ \lambda &\mapsto \exp(\lambda \log u) \end{aligned}.$$

It is easy to see that  $\phi : \mathbb{G}_a \rightarrow \phi(\mathbb{G}_a)$  is an *isomorphism* of algebraic groups (see [H2,15.1]). Moreover,  $u = \phi(1)$ , and so  $V \subseteq \phi(\mathbb{G}_a)$ , where  $V = \overline{\langle u \rangle}$ . Now  $u$  has infinite order which forces  $V$  to have dimension at least 1. But  $\phi(\mathbb{G}_a)$  is connected and 1-dimensional, which forces  $V = \phi(\mathbb{G}_a)$ . Therefore  $u$  lies in a 1-dimensional closed connected abelian unipotent subgroup of  $G$ , namely  $V$  (with  $V \cong \mathbb{G}_a$ ). The situation in positive characteristic is quite different. For then any (non-identity) unipotent element  $u \in G$  has finite order, and so  $\langle u \rangle$  is finite (and closed), which forces  $u \notin 1 = \langle u \rangle^\circ$ . Therefore more elaborate methods are required. However, the methods we shall employ still retain the ‘exponentiation’ theme.

As an obvious generalization of the above corollary, we can ask the following:

**Generalized Problem** Let  $G$  be a reductive algebraic group defined over an algebraically closed field  $K$  of characteristic  $p > 0$ . Let  $1 \neq u \in G_u$  be unipotent, with  $\text{o}(u) = p^t$ ,  $t \in \mathbb{N}$ . Can we find a  $t$ -dimensional closed connected abelian unipotent subgroup  $V$  of  $G$ , with  $u \in V$ ?

If so, this would be the best result, in the sense of ‘minimal dimension’, that we could hope for. Indeed let  $W$  be any  $t$ -dimensional connected unipotent group (*not* necessarily abelian). By the structure theory of connected solvable algebraic groups (see [H2,19.3]), there exists a chain of closed connected subgroups

$$W = W_t \supsetneq W_{t-1} \supsetneq \cdots \supsetneq W_1 \supsetneq W_0 = 1,$$

where  $W_i \trianglelefteq W$ , and  $\dim(W_{i+1}/W_i) = 1$ ,  $0 \leq i \leq t-1$ , which forces  $W_{i+1}/W_i \cong \mathbb{G}_a$  (since  $W_{i+1}/W_i$  is connected and unipotent). Since  $px = 0$  for all  $x \in \mathbb{G}_a$ , it follows that

$$(*) \quad x^{p^t} = 1 \quad \text{for all } x \in W,$$

and so  $W$  cannot contain unipotent elements  $v$  with  $\text{o}(v) = p^i$  and  $i > \dim(W)$ . The smallest power of  $p$  satisfying condition  $(*)$  will be called the *period* of  $W$ , and be denoted by  $\text{per}(W)$ . We have  $\text{per}(W) \leq p^t$ . Our aim is to solve the generalized problem, with as few restrictions on the characteristic as possible. We begin with a study of connected abelian unipotent groups.

# Chapter 1

## Witt Groups and Artin-Hasse Exponentials

Let  $V$  be an  $n$ -dimensional connected abelian unipotent group defined over an algebraically closed field  $K$  of characteristic  $p \geq 0$ . When  $p = 0$ , it can be shown that

$$(*) \quad V \cong \mathbb{G}_a \times \cdots \times \mathbb{G}_a, \quad n \text{ copies.}$$

Now suppose  $p > 0$ . The groups in  $(*)$  all have period  $p$ , and conversely, every connected abelian unipotent group of period  $p$  is isomorphic to a product of groups  $\mathbb{G}_a$  (see [S,VII,2,7;11] and [Sp3,2.6.7]). But this does *not* exhaust all the possibilities. For example, let  $p = 2$  and take  $V$  to be the group of all matrices of the form

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & a \\ 0 & 0 & 1 \end{pmatrix}, \quad a, b \in K.$$

We have

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & a \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & c & d \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+c & b+d+ac \\ 0 & 1 & a+c \\ 0 & 0 & 1 \end{pmatrix}, \quad a, b, c, d \in K.$$

We can reformulate  $V$  as follows: Define a group operation  $\oplus$  on  $K^2$  by

$$(a, b) \oplus (c, d) = (a + c, b + d + ac), \quad a, b, c, d \in K,$$

and write  $W_2(K) = (K^2, \oplus)$ . The ‘additive’ identity is  $0 = (0, 0)$ , and the ‘additive’ inverse of  $(a, b)$  is  $\ominus(a, b) = (a, a^2 + b)$ . Write  $x = (a, b)$  and  $1 = (1, 0)$ , and note that

$$(a, b) \oplus (a, b) = (0, a^2) \text{ and } (0, a^2) \oplus (0, a^2) = (0, 0).$$

Then  $2^2 \cdot x = 0$  and  $2 \cdot 1 \neq 0$ , and so  $W_2(K)$  is a 2-dimensional connected abelian unipotent group of period  $2^2$ . This is an example of what is called a *Witt group*. We have  $W_2(K) \cong V$  (as algebraic groups) under the mapping

$$\begin{array}{ccc} W_2(K) & \rightarrow & V \\ (a, b) & \mapsto & \begin{pmatrix} 1 & a & b \\ 0 & 1 & a \\ 0 & 0 & 1 \end{pmatrix}. \end{array}$$

This construction will be extended in 1.1.

## 1.1 Witt Vectors

In this section we describe the construction of certain rings of vectors associated with a commutative ring with identity. These rings were originally defined by Witt, who used them to study abelian  $p$ -extensions (see [Wi]). However they are also closely related to the study of connected abelian unipotent groups, and will play an important role in our studies. The approach we follow is that given in [K,7] (also see [J4,8.10]).

Let  $p \in \mathbb{N}$  be a fixed prime, and consider the polynomial ring  $A = \mathbb{Q}[X_i, Y_j, Z_k]$ , where  $i, j, k = 0, 1, 2, \dots$ . Write  $A^{\mathbb{N}}$  for the Cartesian product of  $|\mathbb{N} \cup 0|$  copies of  $A$ . The elements of the ring  $A^{\mathbb{N}}$  are infinite *vectors*

$$x = (x_0, x_1, \dots, x_{n-1}, \dots) = (x_i), \quad x_i \in A,$$

where addition (denoted by  $+$ ) and multiplication (denoted by juxtaposition) are performed component-wise, with equality defined in the usual sense. We wish to define a new ring structure on the set  $A^{\mathbb{N}}$ . This will be achieved via the following construction. Let  $x = (x_0, x_1, \dots, x_{n-1}, \dots) \in A^{\mathbb{N}}$ , and write

$$\pi(x) = (x_0^p, x_1^p, \dots, x_{n-1}^p, \dots).$$

Given  $x_0, x_1, \dots, x_{n-1}, \dots \in A$ , we shall define elements  $x^{(0)}, x^{(1)}, \dots, x^{(n-1)}, \dots \in A$  by means of the recursion:

$$x^{(0)} = x_0 \quad \text{and} \quad x^{(i)} = (\pi(x))^{(i-1)} + p^i x_i, \quad i \geq 1. \quad (1)$$

This determines a map  $\phi: A^{\mathbb{N}} \rightarrow A^{\mathbb{N}}$ , where

$$\phi(x_0, x_1, \dots, x_{n-1}, \dots) = (x^{(0)}, x^{(1)}, \dots, x^{(n-1)}, \dots).$$

Calculating the first three terms gives  $x^{(0)} = x_0$ ,

$$\begin{aligned} x^{(1)} &= (\pi(x))^{(0)} + p x_1 \\ &= (x_0^p)_0 + p x_1 \\ &= x_0^p + p x_1, \end{aligned}$$

and

$$\begin{aligned} x^{(2)} &= (\pi(x))^{(1)} + p^2 x_2 \\ &= (x_0^p)^p + p x_1^p + p^2 x_2 \\ &= x_0^{p^2} + p x_1^p + p^2 x_2. \end{aligned}$$

Applying induction to (1), we obtain

$$x^{(0)} = x_0 \text{ and } x^{(i)} = x_0^{p^i} + px_1^{p^{i-1}} + \cdots + p^{i-1}x_{i-1}^p + p^i x_i, \quad i \geq 1. \quad (2)$$

Next let  $x^{(0)}, x^{(1)}, \dots, x^{(n-1)}, \dots \in A$ , and define elements  $x_0, x_1, \dots, x_{n-1}, \dots \in A$  by means of the *inverse* recursion:

$$x_0 = x^{(0)} \text{ and } x_i = \frac{1}{p^i} \left( x^{(i)} - x_0^{p^i} - px_1^{p^{i-1}} - \cdots - p^{i-1}x_{i-1}^p \right), \quad i \geq 1. \quad (3)$$

This determines a map  $\psi : A^{\mathbb{N}} \rightarrow A^{\mathbb{N}}$ , where

$$\psi(x^{(0)}, x^{(1)}, \dots, x^{(n-1)}, \dots) = (x_0, x_1, \dots, x_{n-1}, \dots).$$

A direct calculation shows that  $\psi \circ \phi = \phi \circ \psi = 1$  on  $A^{\mathbb{N}}$ , and so  $\phi$  is bijective with inverse  $\psi$ .

Before defining the new ring structure, we introduce the following useful notation. Given  $x^{(0)}, x^{(1)}, \dots, x^{(n-1)}, \dots \in A$ , we shall define

$$[x^{(0)}, x^{(1)}, \dots, x^{(n-1)}, \dots] = (x_0, x_1, \dots, x_{n-1}, \dots) \in A^{\mathbb{N}},$$

where the  $x_i$ ,  $i = 0, 1, 2, \dots$ , are defined by (3). Sometimes it will be convenient to use the shorthand notation  $[x^{(i)}] = (x_i)$ . Conversely, given the element  $x = (x_0, x_1, \dots, x_{n-1}, \dots) \in A^{\mathbb{N}}$ , we have  $x = [x^{(0)}, x^{(1)}, \dots, x^{(n-1)}, \dots]$ , where the  $x^{(i)}$ ,  $i = 0, 1, 2, \dots$ , are defined by (2). We are now in a position to introduce new binary operations of addition (denoted by  $\oplus$ ) and multiplication (denoted by  $\otimes$ ) on the set  $A^{\mathbb{N}}$ . Let

$$\begin{aligned} x &= (x_0, x_1, \dots, x_{n-1}, \dots) = [x^{(0)}, x^{(1)}, \dots, x^{(n-1)}, \dots], \\ y &= (y_0, y_1, \dots, y_{n-1}, \dots) = [y^{(0)}, y^{(1)}, \dots, y^{(n-1)}, \dots] \end{aligned}$$

be two elements of  $A^{\mathbb{N}}$ . We shall define

$$x \oplus y = [x^{(0)} + y^{(0)}, x^{(1)} + y^{(1)}, \dots, x^{(n-1)} + y^{(n-1)}, \dots] \quad (4)$$

(that is,  $(x \oplus y)^{(i)} = x^{(i)} + y^{(i)}$ ,  $i \geq 0$ ), and

$$x \otimes y = [x^{(0)}y^{(0)}, x^{(1)}y^{(1)}, \dots, x^{(n-1)}y^{(n-1)}, \dots] \quad (5)$$

(that is,  $(x \otimes y)^{(i)} = x^{(i)}y^{(i)}$ ,  $i \geq 0$ ). Note that, in general,  $x \oplus y \neq x + y$  and  $x \otimes y \neq xy$  (see (7) and (8) which follow). We shall write  $W(A)$  for the set  $A^{\mathbb{N}}$  endowed with the operations  $\oplus$  and  $\otimes$  as given above. The fact that  $W(A)$  has the structure of a ring follows from the next result.

**Lemma 1.1.1** [K,7,1]  $W(A)$  is a commutative ring with identity, of characteristic 0, isomorphic to  $A^{\mathbb{N}}$  under the map  $\theta : W(A) \rightarrow A^{\mathbb{N}}$ , where

$$\theta[x^{(0)}, x^{(1)}, \dots, x^{(n-1)}, \dots] = (x^{(0)}, x^{(1)}, \dots, x^{(n-1)}, \dots).$$

**Proof** That  $\theta$  preserves addition and multiplication follows from the definitions (4) and (5) of addition and multiplication in  $W(A)$ . The map is clearly onto  $A^{\mathbb{N}}$ . Now suppose  $\theta(x) = \theta(y)$  with  $x = (x_i) = [x^{(i)}]$ ,  $y = (y_i) = [y^{(i)}] \in W(A)$  (in shorthand notation). Then  $(x^{(i)}) = (y^{(i)})$ , and so  $x^{(i)} = y^{(i)}$  for all  $i \geq 0$ . It follows from (3) that  $x_i = y_i$  for all  $i \geq 0$ . Therefore  $x = y$ , as required.  $\square$

We now determine the zero and identity elements of the ring  $W(A)$ , which we denote by 0 and 1, respectively. Write  $x = (a, 0, \dots, 0, \dots) \in W(A)$ ,  $a \in A$ , then by (2), we have

$$x^{(0)} = a \text{ and } x^{(i)} = a^{p^i} \text{ for } i \geq 1.$$

This gives  $(a, 0, \dots, 0, \dots) = [a, a^p, a^{p^2}, \dots]$ , and so on putting  $a = 0$  and  $a = 1$ , we obtain

$$(0, 0, \dots, 0, \dots) = [0, 0, \dots, 0, \dots] \text{ and } (1, 0, \dots, 0, \dots) = [1, 1, \dots, 1, \dots],$$

respectively. Now by (4) and (5),  $[0, 0, \dots, 0, \dots]$  and  $[1, 1, \dots, 1, \dots]$  are, respectively, the zero and identity elements of  $W(A)$  in  $[\cdot]$  form. Therefore  $0 = (0, 0, \dots, 0, \dots)$  and  $1 = (1, 0, \dots, 0, \dots)$  in  $W(A)$ .

Let  $x = (x_i) \in W(A)$ . We will denote the additive inverse of  $x$  by  $\ominus x$ . Write  $y = (y_i) = \ominus x$ , so that (in the shorthand notation)

$$x \oplus y = [x^{(i)} + y^{(i)}] = 0 = [0].$$

This gives  $y^{(i)} = -x^{(i)}$  for all  $i \geq 0$ , and so it follows from (3) that

$$y_0 = -x^{(0)} \text{ and } y_i = \frac{1}{p^i} \left( -x^{(i)} - y_0^{p^i} - p y_1^{p^{i-1}} - \dots - p^{i-1} y_{i-1}^{p^i} \right), \quad i \geq 1, \quad (6)$$

where  $x^{(i)}$ ,  $i = 0, 1, 2, \dots$ , is given by (2). Using (6), we can determine  $\ominus x$ . For example, let  $x = 1 = (1, 0, \dots, 0, \dots) = [1, 1, \dots, 1, \dots]$ . Then  $x^{(i)} = 1$  for all  $i \geq 0$ , and so

$$(\ominus x)_i = \begin{cases} -1 & : i = 0 \\ -1 & : i \geq 1, p = 2 \\ 0 & : i \geq 1, p > 2 \end{cases}$$



(using  $2^0 + 2^1 + \dots + 2^{i-1} = 2^i - 1$  for the case  $p = 2$ ).

Given  $x, y \in W(A)$ , we now study more closely the elements  $x \oplus y$  and  $x \otimes y$ , and show that their coordinates have certain integrality properties. It is these properties which allow us to define the main objects of this section. To begin with, we concentrate on the elements  $X = (X_0, X_1, X_2, \dots)$ ,  $Y = (Y_0, Y_1, Y_2, \dots) \in W(A)$ . By (4) we have

$$\begin{aligned} X \oplus Y &= [X^{(0)} + Y^{(0)}, X^{(1)} + Y^{(1)}, \dots, X^{(n-1)} + Y^{(n-1)}, \dots] \\ &= ((X \oplus Y)_0, (X \oplus Y)_1, \dots, (X \oplus Y)_{n-1}, \dots), \end{aligned}$$

where by (2) and (3),

$$\begin{aligned} (X \oplus Y)_0 &= X^{(0)} + Y^{(0)} = X_0 + Y_0, \\ (X \oplus Y)_1 &= \frac{1}{p}(X^{(1)} + Y^{(1)} - ((X \oplus Y)_0)^p) \\ &= \frac{1}{p}(X_0^p + pX_1 + Y_0^p + pY_1 - (X_0 + Y_0)^p) \\ &= X_1 + Y_1 + \frac{1}{p}(X_0^p + Y_0^p - (X_0 + Y_0)^p). \end{aligned} \tag{7}$$

It is clear from (7) that  $(X \oplus Y)_1 \neq X_1 + Y_1$ . Next we have, by (5),

$$\begin{aligned} X \otimes Y &= [X^{(0)}Y^{(0)}, X^{(1)}Y^{(1)}, \dots, X^{(n-1)}Y^{(n-1)}, \dots] \\ &= ((X \otimes Y)_0, (X \otimes Y)_1, \dots, (X \otimes Y)_{n-1}, \dots), \end{aligned}$$

where by (2) and (3),

$$\begin{aligned} (X \otimes Y)_0 &= X^{(0)}Y^{(0)} = X_0Y_0, \\ (X \otimes Y)_1 &= \frac{1}{p}(X^{(1)}Y^{(1)} - ((X \otimes Y)_0)^p) \\ &= \frac{1}{p}((X_0^p + pX_1)(Y_0^p + pY_1) - (X_0Y_0)^p) \\ &= X_0^pY_1 + X_1Y_0^p + pX_1Y_1. \end{aligned} \tag{8}$$

It is clear from (8) that  $(X \otimes Y)_1 \neq X_1Y_1$ .

The following notation is required: Let  $R$  be a commutative ring with identity, and  $U$  a subring of  $R$ . For  $a, b \in R$ , we shall write  $a \equiv b \pmod{U}$  whenever  $a - b \in U$ . Now it follows (by induction) from (2), (3), and the definitions (4) and (5), that

$$(X \oplus Y)_i, (X \otimes Y)_i \in \mathbb{Q}[X_0, Y_0, \dots, X_i, Y_i], \quad i \geq 0.$$

Moreover, by (2), (3), and (4), we have

$$(X \oplus Y)_i \equiv \frac{1}{p^i} (X^{(i)} + Y^{(i)}) \pmod{\mathbb{Q}[X_0, Y_0, \dots, X_{i-1}, Y_{i-1}]}, \quad i \geq 1,$$

and

$$X^{(i)} \equiv p^i X_i \pmod{\mathbb{Z}[X_0, \dots, X_{i-1}]}, \quad i \geq 1.$$

Therefore

$$\begin{aligned} (X \oplus Y)_0 &= X_0 + Y_0, \\ (X \oplus Y)_i &= X_i + Y_i + f_i(X_0, Y_0, \dots, X_{i-1}, Y_{i-1}), \quad i \geq 1, \end{aligned} \tag{9}$$

where  $f_i(X_0, Y_0, \dots, X_{i-1}, Y_{i-1}) \in \mathbb{Q}[X_0, Y_0, \dots, X_{i-1}, Y_{i-1}]$ . In fact, the expressions  $(X \oplus Y)_i$  and  $(X \otimes Y)_i$ ,  $i \geq 0$ , are polynomials in  $X_0, Y_0, \dots, X_i, Y_i$  with *integer* coefficients. This is already clear for the cases  $i = 0$  and  $i = 1$  given in (7) and (8). Before we can prove this in general, we need the following

**Lemma 1.1.2** [K,7,1.1] *Let  $j, m \in \mathbb{N}$ , and  $k \in \mathbb{N} \cup 0$  with  $0 \leq k \leq m - 1$ , and let  $x = (x_i)$ ,  $y = (y_i) \in W(A)$  where*

$$x_i, y_i \in \mathbb{Z}[X_0, Y_0, \dots, X_{m-1}, Y_{m-1}] \quad \text{for } 0 \leq i \leq m - 1.$$

*Then the following two conditions are equivalent:*

- (i)  $x_i \equiv y_i \pmod{p^j \mathbb{Z}[X_0, Y_0, \dots, X_{m-1}, Y_{m-1}]}$  for all  $0 \leq i \leq k$ .
- (ii)  $x^{(i)} \equiv y^{(i)} \pmod{p^{i+j} \mathbb{Z}[X_0, Y_0, \dots, X_{m-1}, Y_{m-1}]}$  for all  $0 \leq i \leq k$ .

**Proof** For brevity we write  $\mathbb{Z}[X_r, Y_s]$  for  $\mathbb{Z}[X_0, Y_0, \dots, X_{m-1}, Y_{m-1}]$ . If  $k = 0$  the result is clearly true, since  $x^{(0)} = x_0$  and  $y^{(0)} = y_0$  by (1). Now suppose  $k \geq 1$ . By induction we may assume that (i) and (ii) hold and are equivalent for all  $0 \leq i \leq k - 1$ . Since  $x_i \equiv y_i \pmod{p^j \mathbb{Z}[X_r, Y_s]}$  for  $0 \leq i \leq k - 1$ , and  $\binom{p}{t} \equiv 0 \pmod{p}$  for  $1 \leq t \leq p - 1$ , we obtain

$$x_i^p \equiv y_i^p \pmod{p^{j+1} \mathbb{Z}[X_r, Y_s]}, \quad 0 \leq i \leq k - 1.$$

The induction hypothesis applied to the elements  $\pi(x)$  and  $\pi(y)$ , which clearly satisfy the conditions of the lemma, now gives (for  $i = k - 1$ )

$$\pi(x)^{(k-1)} \equiv \pi(y)^{(k-1)} \pmod{p^{(k-1)+(j+1)} \mathbb{Z}[X_r, Y_s]},$$

and so by (1),

$$x^{(k)} - p^k x_k \equiv y^{(k)} - p^k y_k \pmod{p^{k+j} \mathbb{Z}[X_r, Y_s]}.$$

It follows that

$$\begin{aligned} x_k \equiv y_k \pmod{p^j \mathbb{Z}[X_r, Y_s]} &\Leftrightarrow p^k x_k \equiv p^k y_k \pmod{p^{k+j} \mathbb{Z}[X_r, Y_s]} \\ &\Leftrightarrow x^{(k)} \equiv y^{(k)} \pmod{p^{k+j} \mathbb{Z}[X_r, Y_s]}, \end{aligned}$$

as required.  $\square$

We can now prove the following

**Theorem 1.1.3** [K,7,1.2] *Each  $(X \oplus Y)_i, (X \otimes Y)_i \in \mathbb{Z}[X_0, Y_0, \dots, X_i, Y_i]$ ,  $i = 0, 1, 2, \dots$ .*

**Proof** Write  $\mathbb{Z}[X_r, Y_s]$  for  $\mathbb{Z}[X_0, Y_0, \dots, X_i, Y_i]$ , and let  $X \circ Y$  denote  $X \oplus Y$  or  $X \otimes Y$ . The result is clearly true for  $i = 0$  (see (7) and (8) for example). Now let  $i \geq 1$ . We may assume by induction that

$$(X \circ Y)_k \in \mathbb{Z}[X_0, Y_0, \dots, X_k, Y_k] \subseteq \mathbb{Z}[X_r, Y_s] \text{ for all } 0 \leq k \leq i-1.$$

By (1), we have

$$(*) \quad p^i (X \circ Y)_i = (X \circ Y)^{(i)} - (\pi(X \circ Y))^{(i-1)}.$$

Next we show that

$$(**) \quad (X \circ Y)^{(i)} \equiv (\pi(X) \circ \pi(Y))^{(i-1)} \pmod{p^i \mathbb{Z}[X_r, Y_s]}.$$

By definition (4), we have  $X \oplus Y = [X^{(i)} + Y^{(i)}]$ , and so using (1) we obtain

$$\begin{aligned} (X \oplus Y)^{(i)} &= X^{(i)} + Y^{(i)} = (\pi(X))^{(i-1)} + (\pi(Y))^{(i-1)} + p^i (X_i + Y_i) \\ &= (\pi(X) \oplus \pi(Y))^{(i-1)} + p^i (X_i + Y_i), \end{aligned}$$

and so (\*\*) holds in the case  $\circ = \oplus$ . Now by definition (5), we have  $X \otimes Y = [X^{(i)} Y^{(i)}]$ , and so

$$(X \otimes Y)^{(i)} = X^{(i)} Y^{(i)},$$

whereas

$$\begin{aligned} (\pi(X) \otimes \pi(Y))^{(i-1)} &= \pi(X)^{(i-1)} \pi(Y)^{(i-1)} \\ &= (X^{(i)} - p^i X_i)(Y^{(i)} - p^i Y_i) \\ &= X^{(i)} Y^{(i)} + p^i (p^i X_i Y_i - X_i Y^{(i)} - Y_i X^{(i)}), \end{aligned}$$

using (1). Moreover  $X^{(i)} = X_0^{p^i} + pX_1^{p^{i-1}} + \dots + p^{i-1}X_{i-1}^p + p^iX_i$  by (2), with a similar expression for  $Y^{(i)}$ , and so  $(**)$  holds in the case  $\circ = \otimes$  also.

Now given any  $f \in \mathbb{Z}[X_0, Y_0, \dots, X_k, Y_k]$ ,  $k \in \mathbb{N}$ , we have

$$f(X_0, Y_0, \dots, X_k, Y_k)^p \equiv f(X_0^p, Y_0^p, \dots, X_k^p, Y_k^p) \pmod{p\mathbb{Z}[X_0, Y_0, \dots, X_k, Y_k]}$$

(also see 1.4 which follows). Taking  $f = (X \circ Y)_k \in \mathbb{Z}[X_0, Y_0, \dots, X_k, Y_k]$  for  $0 \leq k \leq i-1$  (by induction hypothesis), we have

$$((X \circ Y)_k)^p = (\pi(X \circ Y))_k \quad \text{and} \quad f(X_0^p, Y_0^p, \dots, X_k^p, Y_k^p) = (\pi(X) \circ \pi(Y))_k,$$

and so

$$(\pi(X \circ Y))_k \equiv (\pi(X) \circ \pi(Y))_k \pmod{p\mathbb{Z}[X_r, Y_s]}, \quad 0 \leq k \leq i-1.$$

Applying 1.1.2 with  $j = 1$ ,  $m = i$ ,  $x = \pi(X \circ Y)$ , and  $y = \pi(X) \circ \pi(Y)$ , we obtain

$$(\pi(X \circ Y))^{(i-1)} \equiv (\pi(X) \circ \pi(Y))^{(i-1)} \pmod{p^i\mathbb{Z}[X_r, Y_s]}.$$

Combining this with  $(**)$  gives  $(\pi(X \circ Y))^{(i-1)} \equiv (X \circ Y)^{(i)} \pmod{p^i\mathbb{Z}[X_r, Y_s]}$ . Finally, it follows from  $(*)$  that  $(X \circ Y)_i \in \mathbb{Z}[X_r, Y_s]$ , as required.  $\square$

Using 1.1.3, we can now write, for  $i \geq 0$ ,

$$\begin{aligned} (X \oplus Y)_i &= A_i(X_r, Y_s) \in \mathbb{Z}[X_r, Y_s], \quad \text{and} \\ (X \otimes Y)_i &= M_i(X_r, Y_s) \in \mathbb{Z}[X_r, Y_s], \quad 0 \leq r, s \leq i. \end{aligned} \tag{10}$$

Now let  $x = (x_i)$ ,  $y = (y_i) \in W(A)$ , be arbitrary. There exists a ring homomorphism  $\theta : A \rightarrow A$  satisfying  $\theta(X_i) = x_i$  and  $\theta(Y_i) = y_i$ , for all  $i \geq 0$  (with  $\theta$  acting as the identity on  $\mathbb{Q}[Z_k]$ ,  $k \geq 0$ ). We have  $\theta(X^{(i)}) = x^{(i)}$  and  $\theta(Y^{(i)}) = y^{(i)}$  (see (2)). Therefore  $\theta((X \oplus Y)^{(i)}) = (x \oplus y)^{(i)}$ , and so  $\theta((X \oplus Y)_i) = (x \oplus y)_i$ , using (3) and induction on  $i$ . Similarly we obtain  $\theta((X \otimes Y)_i) = (x \otimes y)_i$ , and so

$$\begin{aligned} (x \oplus y)_i &= A_i(x_r, y_s), \quad \text{and} \\ (x \otimes y)_i &= M_i(x_r, y_s), \quad 0 \leq r, s \leq i. \end{aligned} \tag{11}$$

We now simplify the notation, by writing  $x + y$  for  $x \oplus y$ , and  $xy$  for  $x \otimes y$ , where  $x, y \in W(A)$ . The integrality properties of (10) are the key to defining the main objects of

this section. Let  $R$  be any commutative ring with identity,  $1 \in R$ , and let  $\phi : \mathbb{Z} \rightarrow R$  be the (natural) homomorphism defined by

$$\phi(0) = 0, \quad \phi(c) = c \cdot 1 = \underbrace{1 + \cdots + 1}_{c \text{ times}}, \quad c \in \mathbb{N}, \quad \text{and} \quad \phi(-c) = -(c \cdot 1).$$

For brevity we shall write  $\phi(c) = \bar{c} = c \cdot 1$ , for *all*  $c \in \mathbb{Z}$ , as this causes no confusion. Now let  $\bar{A}_i(X_r, Y_s)$  and  $\bar{M}_i(X_r, Y_s)$  be the polynomials in  $R[X_r, Y_s]$  obtained from  $A_i(X_r, Y_s)$  and  $M_i(X_r, Y_s)$ , respectively, by replacing each coefficient  $c \in \mathbb{Z}$  by  $\bar{c} = c \cdot 1 \in R$ .

**Definition 1** The *Witt ring*  $W(R)$  of  $R$  is defined to be the set of all infinite *vectors*

$$a = (a_0, a_1, \dots, a_{n-1}, \dots) = (a_i), \quad a_i \in R,$$

with equality defined as usual. Let  $a = (a_i)$ ,  $b = (b_i) \in W(R)$ . Addition and multiplication in  $W(R)$  are defined as follows:

$$\begin{aligned} (a + b)_i &= \bar{A}_i(a_r, b_s), \quad \text{and} \\ (ab)_i &= \bar{M}_i(a_r, b_s), \quad 0 \leq r, s \leq i \end{aligned} \tag{12}$$

(where  $+$  and juxtaposition also denote the addition and multiplication operations of  $R$ ).

**Definition 2** For  $n \geq 1$ , the  $n^{\text{th}}$  *Witt ring*  $W_n(R)$  of  $R$  is defined to be the set of all  $n$ -tuples

$$a = (a_0, a_1, \dots, a_{n-1}) = (a_i), \quad a_i \in R,$$

with equality defined as usual, and addition and multiplication defined as in (12).

We now prove

**Theorem 1.1.4** [K,7,1.3] *The following hold:*

- (i)  $W(R)$  and  $W_n(R)$ ,  $n \geq 1$ , are commutative rings. The zero and identity elements of  $W(R)$  are  $(0, 0, \dots, 0, \dots)$  and  $(1, 0, \dots, 0, \dots)$ , respectively, whilst those of  $W_n(R)$  are  $(0, 0, \dots, 0)$  and  $(1, 0, \dots, 0)$ , respectively.
- (ii) The map  $\sigma_n : W(R) \rightarrow W_n(R)$  given by  $\sigma_n(a) = (a_0, a_1, \dots, a_{n-1})$ ,  $a = (a_i) \in W(R)$ , is a surjective ring homomorphism.

**Proof** (i) Write  $B = \mathbb{Z}[X_i, Y_j, Z_k]$ ,  $i, j, k = 0, 1, 2, \dots$ , a subring of  $A$ . Then  $W(B)$  is the subring of  $W(A)$  consisting of all vectors whose coordinates are in  $B$ . Let  $x = (x_i)$ ,  $y = (y_i)$ , and  $z = (z_i)$  be three fixed elements of  $W(R)$ . Define a map  $\psi : B \rightarrow R$  by

$$\psi(n) = n \cdot 1, \quad n \in \mathbb{Z}, \quad \psi(X_i) = x_i, \quad \psi(Y_i) = y_i, \quad \text{and} \quad \psi(Z_i) = z_i,$$

and extend this to a ring homomorphism. The map  $\psi$  induces a map  $\psi_W : W(B) \rightarrow W(R)$ , where

$$\psi_W(a_i) = (\psi(a_i)), \quad a_i \in B.$$

Let  $a = (a_i)$ ,  $b = (b_i) \in W(B)$ . By (11) we have

$$a + b = ((a + b)_i) = (A_i(a_r, b_s)), \quad 0 \leq r, s \leq i,$$

and so

$$\begin{aligned} \psi_W(a + b) &= (\psi(A_i(a_r, b_s))) \\ &= (\bar{A}_i(\psi(a_r), \psi(b_s))) \quad (\text{by the definition of } \psi) \\ &= (\psi(a_i)) + (\psi(b_i)) \quad (\text{by (12)}) \\ &= \psi_W(a) + \psi_W(b). \end{aligned}$$

Therefore  $\psi_W$  preserves addition. We can show similarly that  $\psi_W$  preserves multiplication. Moreover, we have

$$\psi_W(X) = x, \quad \psi_W(Y) = y, \quad \text{and} \quad \psi_W(Z) = z,$$

where  $X = (X_i)$ ,  $Y = (Y_i)$ , and  $Z = (Z_i)$ . Since  $W(B)$  is a commutative ring, it follows from this that  $W(R)$  is a commutative ring. Now we have

$$\psi_W(0, 0, \dots, 0, \dots) = (0, 0, \dots, 0, \dots) \quad \text{and} \quad \psi_W(1, 0, \dots, 0, \dots) = (1, 0, \dots, 0, \dots),$$

which shows that the zero and identity elements of  $W(R)$  are as stated. Almost identical arguments can be used to obtain the results concerning  $W_n(R)$ ,  $n \geq 1$ .

(ii) The map  $\sigma_n$  is clearly onto, and is a homomorphism by virtue of (12). □

Let  $R, S$  be commutative rings with identity, and suppose  $\phi : R \rightarrow S$  is a *unital* ring homomorphism (that is,  $\phi(1) = 1$ ). Then it follows from (12) that the induced map  $\phi_W : W(R) \rightarrow W(S)$ , given by  $\phi_W(a_i) = (\phi(a_i))$ ,  $a_i \in R$ , is a (unital) ring homomorphism. An analogous result holds for  $W_n(R)$  and  $W_n(S)$ ,  $n \geq 1$ .

We end this section by determining the additive inverse of  $x = (x_i) \in W(R)$ . Refer to (12) and above for notation. Let  $y = (y_i) = -x$ . By (9) we have  $A_0(X_0, Y_0) = (X + Y)_0 = X_0 + Y_0$ , and so  $y_0 = -x_0$ . Now suppose  $i \geq 1$ , then (9) gives

$$A_i(X_r, Y_s) = (X + Y)_i = X_i + Y_i + f_i(X_0, Y_0, \dots, X_{i-1}, Y_{i-1}), \quad 0 \leq r, s \leq i,$$

where  $f_i(X_0, Y_0, \dots, X_{i-1}, Y_{i-1}) \in \mathbb{Z}[X_0, Y_0, \dots, X_{i-1}, Y_{i-1}]$  by 1.1.3. On replacing each coefficient  $c \in \mathbb{Z}$  by  $\bar{c} = c \cdot 1 \in R$ , we obtain

$$\bar{A}_i(X_r, Y_s) = X_i + Y_i + \bar{f}_i(X_0, Y_0, \dots, X_{i-1}, Y_{i-1}),$$

where  $\bar{f}_i$  has the obvious meaning. Since  $0 = (0, 0, \dots, 0, \dots)$  in  $W(R)$ , it follows that

$$0 = \bar{A}_i(x_r, y_s) = x_i + y_i + \bar{f}_i(x_0, y_0, \dots, x_{i-1}, y_{i-1}),$$

and so we have

$$y_0 = -x_0 \quad \text{and} \quad y_i = -x_i - \bar{f}_i(x_0, y_0, \dots, x_{i-1}, y_{i-1}), \quad i \geq 1.$$

From this we can determine  $-x$ . Moreover, for each  $i \geq 0$ , there exists a fixed polynomial  $P_i(X_0, X_1, \dots, X_i) \in R[X_0, X_1, \dots, X_i]$ , satisfying

$$(-x)_i = P_i(x_0, x_1, \dots, x_i), \tag{13}$$

for all  $x = (x_i) \in W(R)$  (use induction on  $i$ ). This fact will be used in the next section. Note that the same methods clearly apply to  $W_n(R)$ ,  $n \geq 1$ . When  $p$  is *odd* we can be more specific. Indeed it follows from (6) (applied to  $X = (X_i)$ ) and the proof of 1.1.4 that  $(-x)_i = -x_i$ , for all  $i \geq 0$ . Also see [K, 7, 1.4(c)]. If  $p = 2$  the polynomials arising are more complicated.

## 1.2 Witt Groups and Connected Abelian Unipotent Groups

In this section we consider the important case where  $R = K$ , an algebraically closed field of characteristic  $p > 0$ . We show that the Witt rings  $W_n(K)$ ,  $n \geq 1$ , have the natural structure of connected abelian unipotent algebraic groups. We also consider certain useful morphisms between these groups. Finally we briefly discuss how the structure of an *arbitrary* connected abelian unipotent group is connected to the theory of Witt groups.

For brevity, write  $W_n$  for the  $n^{\text{th}}$  Witt ring  $W_n(K)$ ,  $n \in \mathbb{N}$ . The elements of  $W_n$  are  $n$ -tuples  $(x_0, \dots, x_{n-1})$ ,  $x_i \in K$ , and so, as a set,  $W_n = K^n$ . Now  $W_n$  is an additive abelian group under  $+$ , and it follows from (12) and (13) that the maps

$$\begin{array}{ccc} \pi : W_n \times W_n & \rightarrow & W_n \\ (x, y) & \mapsto & x + y \end{array} \quad \text{and} \quad \begin{array}{ccc} i : W_n & \rightarrow & W_n \\ x & \mapsto & -x \end{array}$$

are morphisms of affine varieties  $K^{2n} \rightarrow K^n$  and  $K^n \rightarrow K^n$ , respectively. Therefore  $W_n$  is an  $n$ -dimensional connected abelian (affine) algebraic group. Before showing that  $W_n$  is *unipotent*, we need a couple of lemmas (refer to 1.1 for notation). Throughout  $p$  denotes a fixed prime in  $\mathbb{N}$ .

**Lemma 1.2.1** [K,7,1.6] *Let  $X = (X_i) \in W(A)$ , then*

$$(pX)_i \equiv (s\pi(X))_i \pmod{p\mathbb{Z}[X]} \text{ for all } i \geq 0,$$

*where  $s : W(A) \rightarrow W(A)$  is the (shift) mapping  $a = (a_i) \mapsto (0, a_0, a_1, a_2, \dots)$ .*

**Proof** Let  $a = (a_i) \in W(A)$ , and write  $b = (b_i) = s(a) = (0, a_0, a_1, a_2, \dots)$ . Then using (2), we obtain  $b^{(0)} = b_0 = 0$ , and

$$\begin{aligned} b^{(i)} &= b_0^{p^i} + pb_1^{p^{i-1}} + p^2b_2^{p^{i-2}} + \dots + p^ib_i \\ &= 0 + p(a_0^{p^{i-1}} + pa_1^{p^{i-2}} + \dots + p^{i-1}a_{i-1}) \\ &= pa^{(i-1)}, \quad i \geq 1. \end{aligned}$$

Therefore  $s(a) = [0, pa^{(0)}, pa^{(1)}, pa^{(2)}, \dots]$ , which gives

$$s\pi(X) = [0, p(\pi(X))^{(0)}, p(\pi(X))^{(1)}, p(\pi(X))^{(2)}, \dots],$$



and so

$$(*) \quad (s\pi(X))^{(i)} = \begin{cases} 0 & : i = 0 \\ p(\pi(X))^{(i-1)} & : i \geq 1 \end{cases}.$$

Now by (1) and (4),  $(pX)^{(0)} = pX^{(0)} = pX_0$ , and  $(pX)^{(i)} = pX^{(i)} = p(\pi(X)^{(i-1)} + p^i X_i)$  for  $i \geq 1$ . It follows from (\*) that

$$(pX)^{(i)} \equiv (s\pi(X))^{(i)} \pmod{p^{i+1}\mathbb{Z}[X_i]} \text{ for all } i \geq 0.$$

Let  $m \in \mathbb{N}$  and  $i \in \mathbb{N} \cup 0$  with  $0 \leq i \leq m-1$ , then  $(pX)_i, (s\pi(X))_i \in \mathbb{Z}[X_0, \dots, X_i] \subseteq \mathbb{Z}[X_0, \dots, X_{m-1}]$  (for the former, see (10)). Let  $0 \leq k \leq m-1$ , and apply 1.1.2 to obtain

$$(pX)_i \equiv (s\pi(X))_i \pmod{p\mathbb{Z}[X_0, \dots, X_{m-1}]} \text{ for } 0 \leq i \leq k.$$

Since  $m \geq i+1$  is arbitrary, we must have

$$(pX)_i \equiv (s\pi(X))_i \pmod{p\mathbb{Z}[X]} \text{ for all } i \geq 0,$$

as required. □

Before coming to the second lemma, we need to define some new maps. Let  $R$  be a commutative ring (with identity), and consider the following *shift* mappings:

$$\begin{aligned} s : W(R) &\rightarrow W(R) \\ a = (a_i) &\mapsto (0, a_0, a_1, a_2, \dots) \end{aligned},$$

and for  $n \geq 2$ ,

$$\begin{aligned} s_n : W_n(R) &\rightarrow W_n(R) \\ a = (a_0, a_1, \dots, a_{n-1}) &\mapsto (0, a_0, a_1, \dots, a_{n-2}) \end{aligned},$$

with  $s_1(a_0) = (0)$  for the case  $n = 1$ . It can be shown that  $s$  and  $s_n$ ,  $n \geq 1$ , preserve *addition* (see [K,7,1.4]). However we shall not need these facts here.

We also require the following  $p^{\text{th}}$ -power mappings:

$$\begin{aligned} \pi : W(R) &\rightarrow W(R) \\ a = (a_i) &\mapsto (a_0^p, a_1^p, a_2^p, \dots) \end{aligned},$$

and for  $n \geq 1$ ,

$$\begin{aligned} \pi_n : W_n(R) &\rightarrow W_n(R) \\ a = (a_0, a_1, \dots, a_{n-1}) &\mapsto (a_0^p, a_1^p, \dots, a_{n-1}^p) \end{aligned}.$$

If  $R$  has characteristic  $p$ , then the map  $\lambda \mapsto \lambda^p$ , for all  $\lambda \in R$ , is a unital ring homomorphism. It follows that  $\pi$  and  $\pi_n$ ,  $n \geq 1$ , are both ring homomorphisms (see the remarks after 1.1.4; also see [K,7,1.6]). We now have the following

**Lemma 1.2.2** [K,7,1.6] *Let  $R$  be a commutative ring with identity,  $1 \in R$ , of characteristic  $p$ , and let  $n \geq 1$ . Then the following hold:*

(i)  $p^i y = s^i(\pi^i(y))$  and  $p^i x = s_n^i(\pi_n^i(x))$  for all  $y \in W(R)$ ,  $x \in W_n(R)$ , and  $i \geq 1$ .

(ii) In  $W_n(R)$  we have  $p^n 1 = 0$  and  $p^m 1 \neq 0$ ,  $m < n$ .

**Proof** (i) Let  $y = (y_i) \in W(R)$ . Define  $C = \mathbb{Z}[X_i]$ ,  $i = 0, 1, 2, \dots$ , a subring of  $A$ . Let  $\psi : C \rightarrow R$  denote the (unital) ring homomorphism satisfying  $\psi(X_i) = y_i$ ,  $i \geq 0$ , and  $\psi(n) = n \cdot 1$ ,  $n \in \mathbb{Z}$ . This induces a ring homomorphism  $\psi_W : W(C) \rightarrow W(R)$ , where  $\psi_W(a_i) = (\psi a_i)$ , for all  $(a_i) \in W(C)$ . Now

$$\begin{aligned} py &= \psi_W(pX) = (\psi(pX))_i \\ &= (\psi(s\pi(X)))_i \quad (\text{using 1.2.1}) \\ &= ((s\pi(y)))_i, \end{aligned}$$

and so

$$(*) \quad py = s\pi(y).$$

Now let  $i \geq 2$ , and assume by induction that  $p^{i-1}y = s^{i-1}(\pi^{i-1}(y))$ . It is clear that  $s\pi = \pi s$ , which gives  $(s\pi)^j = s^j\pi^j$  for all  $j \geq 1$ , and so

$$\begin{aligned} p^i y &= p(p^{i-1}y) = ps^{i-1}(\pi^{i-1}(y)) \\ &= p(s\pi)^{i-1}(y) \\ &= (s\pi)^i(y) \quad (\text{using } (*)) \\ &= s^i(\pi^i(y)). \end{aligned}$$

Therefore  $p^i y = s^i(\pi^i(y))$  for all  $i \geq 1$ . Now for  $a = (a_i) \in W(R)$ , we have

$$\sigma_n s(a) = s_n(a_0, a_1, \dots, a_{n-1}).$$

By 1.1.4(ii),  $\sigma_n$  is additive, and so we obtain

$$\begin{aligned} p\sigma_n(y) &= \sigma_n(py) = \sigma_n(s\pi(y)) \\ &= s_n\pi_n(y_0, y_1, \dots, y_{n-1}). \end{aligned}$$

It follows that  $px = s_n(\pi_n(x))$  for all  $x = (x_0, x_1, \dots, x_{n-1}) \in W_n(R)$ , from which we obtain  $p^i x = s_n^i(\pi_n^i(x))$ , for all  $i \geq 1$ , as before.

(ii) Recall that  $1 = (1, 0, \dots, 0)$  in  $W_n(R)$  (see 1.1.4(i)). From part (i) we have

$$p^i 1 = s_n^i(\pi_n^i(1)) = s_n^i(1),$$

and so  $p^n 1 = 0$ , with  $p^m 1 \neq 0$  for  $m < n$ , as required.  $\square$

It follows from 1.2.2(ii) that each element of  $W_n$  has *additive* order a power of  $p$ , and so  $W_n$  is a *unipotent* group. Moreover, we have  $\text{per}(W_n) = p^n$ . The next result is a consequence of 1.2.2.

**Corollary 1.2.3** *Let  $K$  be a field of characteristic  $p$ , and let  $x = (x_0, x_1, \dots, x_{t-1}) \in W_t(K)$ ,  $t \geq 1$ . Then the following hold:*

$$(a) \quad o(x) = p^0 = 1 \quad \Leftrightarrow \quad x = (0, 0, \dots, 0).$$

$$(b) \quad o(x) = p^i, \quad 1 \leq i \leq t-1 \quad \Leftrightarrow \quad x_0 = x_1 = \dots = x_{t-(i+1)} = 0, \quad x_{t-i} \neq 0.$$

$$(c) \quad o(x) = p^t \quad \Leftrightarrow \quad x_0 \neq 0.$$

**Proof** Part (a) is obvious, so assume  $o(x) = p^i$ , where  $1 \leq i \leq t$ . The case  $t = 1$  is clear, so we can further assume  $t \geq 2$ . By 1.2.2(i) we have

$$p^j x = s_t^j(\pi_t^j(x)), \quad 0 \leq j \leq t$$

(on taking  $s_t^0 = \pi_t^0 = 1$  on  $W_t(K)$ ). Setting  $j = i-1$ , we obtain

$$(*)_1 \quad p^{i-1} x = (\underbrace{0, 0, \dots, 0}_{i-1 \text{ elements}}, x_0^{p^{i-1}}, x_1^{p^{i-1}}, \dots, x_{t-i}^{p^{i-1}}) \neq 0.$$

Moreover, for  $1 \leq i \leq t-1$ , we have

$$(*)_2 \quad p^i x = (\underbrace{0, 0, \dots, 0}_i, x_0^{p^i}, x_1^{p^i}, \dots, x_{t-(i+1)}^{p^i}) = 0.$$

Since  $K$  is a field, it follows from  $(*)_2$  that  $x_0 = x_1 = \dots = x_{t-(i+1)} = 0$ . Then  $(*)_1$  gives  $x_{t-i} \neq 0$ , and so (b) follows. Setting  $i = t$  in  $(*)_1$  gives  $x_0 \neq 0$ , from which (c) follows.  $\square$

We now turn our attention to a study of certain morphisms between Witt groups.

**Lemma 1.2.4** *Let  $K$  be an algebraically closed field of characteristic  $p$ , and suppose  $\lambda = (\lambda_0, \lambda_1, \dots, \lambda_{t-1}) \in W_t(K)$ ,  $t \geq 1$ , is arbitrary. Then the following hold:*

(i) *The map*

$$\begin{aligned} \phi_\lambda : W_t(K) &\rightarrow W_t(K) \\ x &\mapsto \lambda x \end{aligned}$$

*is a morphism of algebraic groups.*

(ii) *Let  $a = (a_i)$ ,  $b = (b_i) \in W_t(K)$  be two fixed elements, and suppose  $a_0 \neq 0$ . Then there exists a unique element  $\lambda \in W_t(K)$  such that  $\phi_\lambda(a) = b$  (where  $\phi_\lambda$  is defined as in part (i)).*

**Proof** (i) Let  $x, y \in W_t(K)$  then  $\phi_\lambda(x + y) = \lambda(x + y) = \lambda x + \lambda y = \phi_\lambda(x) + \phi_\lambda(y)$ , using the fact that  $W_t(K)$  is a ring. Now define  $P_i(X_s) = \overline{M}_i(\lambda_r, X_s) \in K[X_s]$ ,  $0 \leq r, s \leq i$ ,  $0 \leq i \leq t - 1$  (see (12)). Then we have

$$(\lambda x)_i = P_i(x_s), \quad 0 \leq s \leq i, \quad 0 \leq i \leq t - 1,$$

and so  $\phi_\lambda$  is a morphism of algebraic groups.

(ii) First consider  $X = (X_i)$ ,  $Y = (Y_i) \in W(A)$ . We have, by (5),

$$XY = [X^{(0)}Y^{(0)}, X^{(1)}Y^{(1)}, \dots] = ((XY)_0, (XY)_1, \dots).$$

Using (2) and (3) we obtain

$$(XY)_0 = X^{(0)}Y^{(0)} = X_0Y_0,$$

and for  $i \geq 1$ ,

$$(XY)_i = \frac{1}{p^i} \left( X^{(i)}Y^{(i)} - (XY)_0^{p^i} - p(XY)_1^{p^{i-1}} - \dots - p^{i-1}(XY)_{i-1}^p \right).$$

Now by (2),

$$X^{(i)}Y^{(i)} = \left( X_0^{p^i} + pX_1^{p^{i-1}} + \dots + p^{i-1}X_{i-1}^p + p^iX_i \right) \left( Y_0^{p^i} + pY_1^{p^{i-1}} + \dots + p^{i-1}Y_{i-1}^p + p^iY_i \right).$$

We can rewrite this in the form

$$X^{(i)}Y^{(i)} = p^i \left( X_0^{p^i}Y_i + X_iY_0^{p^i} \right) + p^{i+1}Q_1 + Q_2,$$

where  $Q_1 \in \mathbb{Z}[X_1, Y_1, \dots, X_i, Y_i]$  and  $Q_2 \in \mathbb{Z}[X_0, Y_0, \dots, X_{i-1}, Y_{i-1}]$ . Therefore, for  $i \geq 1$ , we have

$$(XY)_i = X_0^{p^i} Y_i + X_i Y_0^{p^i} + pQ_1 + \frac{1}{p^i} \left( Q_2 - (XY)_0^{p^i} - p(XY)_1^{p^{i-1}} - \dots - p^{i-1} (XY)_{i-1}^p \right).$$

Write  $R_i = (Q_2 - (XY)_0^{p^i} - p(XY)_1^{p^{i-1}} - \dots - p^{i-1} (XY)_{i-1}^p) / p^i$ , then by 1.1.3,

$$R_i = R_i(X_0, Y_0, \dots, X_{i-1}, Y_{i-1}) \in \mathbb{Z}[X_0, Y_0, \dots, X_{i-1}, Y_{i-1}].$$

Now let  $\lambda = (\lambda_i) \in W_t(K)$ . It follows from (8) and (12) that

$$(*_1) \quad (\lambda a)_0 = \lambda_0 a_0,$$

and for  $1 \leq i \leq t-1$ ,

$$(*_2) \quad (\lambda a)_i = \lambda_0^{p^i} a_i + \lambda_i a_0^{p^i} + \overline{R}_i(\lambda_0, a_0, \dots, \lambda_{i-1}, a_{i-1})$$

(where, as usual,  $\overline{R}_i$  is the polynomial obtained from  $R_i$  by replacing each coefficient  $c \in \mathbb{Z}$  by  $\bar{c} = c \cdot 1$  in the prime subfield of  $K$ ). Using  $(*_1)$  and  $(*_2)$  we can now inductively define a unique element  $\lambda \in W_t(K)$  satisfying  $\lambda a = b$ , as follows:

$$\lambda_0 = b_0 a_0^{-1},$$

and for  $1 \leq i \leq t-1$ ,

$$\lambda_i = \left( b_i - \lambda_0^{p^i} a_i - \overline{R}_i(\lambda_0, a_0, \dots, \lambda_{i-1}, a_{i-1}) \right) \left( a_0^{p^i} \right)^{-1}.$$

The result follows. □

For an alternative proof of 1.2.4(ii), consult [K,7,1.10]. It is worth noting that the map  $\phi_\lambda$  defined in 1.2.4 is an (algebraic) automorphism of  $W_t(K)$  if and only if  $\lambda_0 \neq 0$ . For  $t = 1$  we recover the (well-known) automorphisms  $\phi_\lambda : \mathbb{G}_a \rightarrow \mathbb{G}_a$ , given by  $\phi_\lambda(x) = \lambda x$ , where  $\lambda \in \mathbb{G}_m$ . The final result in this section will be needed in chapter 3.

**Lemma 1.2.5** *Let  $K$  be an algebraically closed field of characteristic  $p$ , and suppose  $a = (a_0, a_1, \dots, a_{t-1}) \in W_t(K)$ ,  $b = (b_0, b_1, \dots, b_{s-1}) \in W_s(K)$ ,  $1 \leq s \leq t$ , with  $\text{o}(a) = p^t$ . Then there exists a morphism of algebraic groups*

$$\psi : W_t(K) \rightarrow W_s(K)$$

*satisfying  $\psi(a) = b$ .*

**Proof** Consider the map

$$\begin{aligned} f_{st} : W_t(K) &\rightarrow W_s(K) \\ x = (x_0, x_1, \dots, x_{t-1}) &\mapsto x' = (x_0, x_1, \dots, x_{s-1}) \end{aligned}$$

Using (12) it is easy to see that  $f_{st}(x + y) = f_{st}(x) + f_{st}(y)$  (also see [K,7,1.3]). Therefore  $f_{st}$  is a (surjective) morphism of algebraic groups. Now  $f_{st}(a) = a' = (a_0, a_1, \dots, a_{s-1})$ , where  $a_0 \neq 0$  (see 1.2.3(c)). By 1.2.4(i) and (ii), there exists a unique  $\lambda \in W_s(K)$ , and a morphism of algebraic groups

$$\begin{aligned} \phi_\lambda : W_s(K) &\rightarrow W_s(K) \\ x &\mapsto \lambda x \end{aligned}$$

satisfying  $\phi_\lambda(a') = b$  (if  $b_0 \neq 0$  then  $\phi_\lambda$  is an automorphism of algebraic groups). Consider the composition map  $\psi = \phi_\lambda \circ f_{st}$ :

$$\begin{aligned} W_t(K) &\xrightarrow{f_{st}} W_s(K) \xrightarrow{\phi_\lambda} W_s(K) \\ x &\mapsto x' \mapsto \lambda x' \end{aligned}$$

It is clear that  $\psi$  is a morphism of algebraic groups, satisfying  $\psi(a) = b$ , as required.  $\square$

We now briefly indicate to what extent the Witt groups classify the set of all connected abelian unipotent groups (for more details, and proofs, see [S,VII,2]). Let  $V$  be an  $n$ -dimensional connected abelian unipotent group. Then the following two conditions are equivalent:

- (i)  $\text{per}(V) = p^n$
- (ii) there exists an isogeny  $\phi : W_n \rightarrow V$

(an *isogeny* is a surjective morphism of algebraic groups with finite kernel). When  $\text{per}(V) \neq p^n$ , instead of the group  $W_n$  above, we have a *product* of Witt groups  $W_{n_1} \times \dots \times W_{n_r}$ , where the integers  $n_i$  are uniquely determined (up to order). All the groups we construct will in fact be *isomorphic* to some  $W_n$ . Although this classification describes, up to isogeny, the structure of every  $n$ -dimensional connected abelian unipotent group of period  $p^n$ , we still do not have a method for constructing such groups inside our given reductive group  $G$ . This will be dealt with in sections 3 – 7.

### 1.3 The Functional Equation Lemma

In this section we develop the necessary tools for constructing the groups described in the previous section. Essentially we generalize the exponentiation approach used in the characteristic 0 case (see p.2). Our account is a simplified version of that given in [Ha,1,2].

We begin with some remarks on formal power series rings. For more details, consult [B1,IV,4], [Ha,A], and [ZS,VII]. Let  $R$  be a commutative ring with identity,  $1 \in R$ , and let  $T$  be an indeterminate. The *formal power series ring*  $R[[T]]$ , with respect to the indeterminate  $T$ , is defined to be the set of all formal sums

$$f(T) = \sum_{n=0}^{\infty} a_n T^n, \quad a_n \in R,$$

where  $T^0 = 1$ , with addition (denoted by  $+$ ) and multiplication (denoted by juxtaposition) defined by

$$\begin{aligned} \sum_{n=0}^{\infty} a_n T^n + \sum_{n=0}^{\infty} b_n T^n &= \sum_{n=0}^{\infty} (a_n + b_n) T^n \\ \left( \sum_{n=0}^{\infty} a_n T^n \right) \left( \sum_{n=0}^{\infty} b_n T^n \right) &= \sum_{n=0}^{\infty} c_n T^n, \quad c_n = \sum_{i+j=n} a_i b_j = \sum_{k=0}^n a_k b_{n-k} \end{aligned}$$

(where  $+$  and juxtaposition also denote the addition and multiplication in  $R$ , respectively). This gives  $R[[T]]$  the structure of a commutative ring with identity element 1 ( $R$  being viewed as a subring of  $R[[T]]$ ). Let  $R[[T]]_0$  be the subring of  $R[[T]]$  consisting of all power series with zero *constant term* (that is,  $a_0 = 0$  in the notation above). Given  $f(T) = \sum_{n=0}^{\infty} a_n T^n \in R[[T]]$  and  $g(T) = \sum_{m=1}^{\infty} b_m T^m \in R[[T]]_0$ , we can *substitute*  $g(T)$  for  $T$  in  $f(T)$  to obtain the *composite power series*

$$(f \circ g)(T) = f(g(T)) = \sum_{n=0}^{\infty} a_n \left( \sum_{m=1}^{\infty} b_m T^m \right)^n = \sum_{n=0}^{\infty} d_n T^n,$$

where  $d_i$ ,  $i \geq 0$ , is the coefficient of  $T^i$  of the power series

$$\sum_{n=0}^i a_n \left( \sum_{m=1}^{\infty} b_m T^m \right)^n.$$

Thus we have polynomials  $Q_0(X_0) = X_0$  and  $Q_n(X_i, Y_j) \in P[X_i, Y_j]$ ,  $n \geq 1$ ,  $1 \leq i, j \leq n$ , where  $P$  is the prime subring of  $R$ , satisfying

$$(f \circ g)(T) = Q_0(a_0) + \sum_{n=1}^{\infty} Q_n(a_i, b_j) T^n,$$

for all  $f(T) = \sum_{n=0}^{\infty} a_n T^n \in R[[T]]$  and  $g(T) = \sum_{m=1}^{\infty} b_m T^m \in R[[T]]_0$ . The following three properties hold: Let  $f(T), \hat{f}(T) \in R[[T]]$  and  $g(T), h(T) \in R[[T]]_0$ . Then

$$\begin{aligned}(f \circ g) \circ h &= f \circ (g \circ h) \\ (f + \hat{f}) \circ g &= (f \circ g) + (\hat{f} \circ g) \quad , \\ (f\hat{f}) \circ g &= (f \circ g)(\hat{f} \circ g)\end{aligned}$$

where, for brevity, we have omitted the indeterminate  $T$ . So, for example,  $f + \hat{f}$  stands for  $f(T) + \hat{f}(T)$ , and  $f\hat{f}$  for  $f(T)\hat{f}(T)$ . For the first property, see [B1,IV,4.3]; for the latter two, see [ZS,VII,1].

Now let  $\sigma : R \rightarrow R$  be a unital ring endomorphism. For  $f(T) = \sum_{n=0}^{\infty} a_n T^n \in R[[T]]$ , define

$$f^\sigma(T) = \sum_{n=0}^{\infty} \sigma(a_n) T^n \in R[[T]].$$

Now let  $g(T) \in R[[T]]_0$ . Since  $\sigma$  is a ring homomorphism, we obtain

$$(f \circ g)^\sigma(T) = (f^\sigma \circ g^\sigma)(T) \quad (14)$$

(also see [Ha,1,2.4]).

Finally let  $f(T) = \sum_{n=1}^{\infty} a_n T^n \in R[[T]]_0$ , with  $a_1$  *invertible* in  $R$  (that is,  $a_1 a_1^{-1} = 1$  for some unique  $a_1^{-1} \in R$ ). Then there exists a unique power series  $f^{-1}(T) = \sum_{n=1}^{\infty} \hat{a}_n T^n \in R[[T]]_0$ , called the *inverse function* power series, such that

$$(f^{-1} \circ f)(T) = T = (f \circ f^{-1})(T)$$

(see [Ha,A.4]). Note that  $\hat{a}_1 = a_1^{-1}$ .

Let  $R$  and  $\sigma$  be as above, and  $U$  a subring of  $R$ . For  $x \in R$  define  $xU = \{xu : u \in U\} \subseteq R$ . Now let  $S$  be a subring of  $R$ , with  $1 \in S$ . Suppose we are given  $r \in R$  and a prime  $p \in \mathbb{N}$  such that the following two conditions are satisfied:

$$\begin{aligned}(\text{FE1}) \quad & \sigma(a) \equiv a^p \pmod{pS} \text{ for all } a \in S \\ (\text{FE2}) \quad & rpS \subseteq S\end{aligned}$$

(where  $pS = (p1)S$  and  $rpS = r(pS)$ ). The ‘mod’ notation was introduced on p.9. Note that (FE1) implies that  $\sigma(S) \subseteq S$ , and so  $\sigma(pS) = p\sigma(S) \subseteq pS$ . The following property also holds



for all  $x \in R$ :

$$xpS \subseteq pS \Rightarrow \sigma(x)pS \subseteq pS. \quad (15)$$

Indeed let  $\sigma(x)pa \in \sigma(x)pS$ ,  $a \in S$ . Since  $1 \in S$ , we have  $px = xp1 \in xpS \subseteq pS$ . Therefore  $p\sigma(x) = \sigma(px) \in \sigma(pS) \subseteq pS$ , and so  $\sigma(x)pa \in pSa \subseteq pS$  as required.

Now let  $g(T) = \sum_{n=1}^{\infty} b_n T^n \in S[[T]]_0$ . We can define a new power series  $f_g(T) = \sum_{n=1}^{\infty} a_n T^n \in R[[T]]_0$  recursively as follows: Write  $n = p^i m$ , where  $i \in \mathbb{N} \cup 0$ , and  $m \in \mathbb{N}$  with  $(m, p) = 1$ , then take

$$a_n = \begin{cases} b_n & : i = 0 \\ b_n + r\sigma(a_{n/p}) & : i \geq 1 \end{cases}. \quad (16)$$

It follows from (16) that  $\sum_{n=1}^{\infty} a_n T^n = \sum_{n=1}^{\infty} b_n T^n + r \sum_{j=1}^{\infty} \sigma(a_j) T^{jp}$ , and so

$$f_g(T) = g(T) + r f_g^\sigma(T^p) \quad (17)$$

(where  $f_g^\sigma(T^p) = (f_g^\sigma \circ T^p)(T)$ , but we use the former notation as it is clearer). Equation (17) is known as a *functional equation*.

Before proving the main result of this section (1.3.4), we require the following three lemmas. For the remainder of this section we choose  $R$ ,  $S$ ,  $\sigma$ , and  $p$  as above. In particular, (FE1) and (FE2) hold.

**Lemma 1.3.1** [Ha,1,2.4.1] *Let  $g(T) = \sum_{n=1}^{\infty} b_n T^n \in S[[T]]_0$  and write  $f_g(T) = \sum_{n=1}^{\infty} a_n T^n$ . Suppose  $n = p^i m$ , where  $i \in \mathbb{N} \cup 0$ , and  $m \in \mathbb{N}$  with  $(m, p) = 1$ . Then*

$$a_n p^i S \subseteq S.$$

**Proof** First suppose  $i = 0$ , then (16) gives  $a_n = b_n \in S$ , and so  $a_n S \subseteq S$ . Now suppose  $i \geq 1$ , so that (16) gives  $a_n = b_n + r\sigma(a_{n/p})$ . Since  $n/p = p^{i-1}m$ , we may assume by induction (on  $i$ ) that

$$a_{n/p} p^{i-1} S \subseteq S.$$

Then  $(p^{i-1} a_{n/p}) p S = a_{n/p} p^i S \subseteq pS$ , and so by (15) we have  $\sigma(p^{i-1} a_{n/p}) p S \subseteq pS$ ; that is,

$\sigma(a_{n/p})p^i S \subseteq pS$ . Using (FE2) we obtain  $r\sigma(a_{n/p})p^i S \subseteq rpS \subseteq S$ . Therefore

$$\begin{aligned} a_n p^i S &= (b_n + r\sigma(a_{n/p}))p^i S \\ &\subseteq b_n p^i S + r\sigma(a_{n/p})p^i S \\ &\subseteq S \end{aligned}$$

(since  $b_n \in S$ ), as required.  $\square$

Before coming to the second lemma, we introduce the following notation: Let  $f(T) = \sum_{n=0}^{\infty} a_n T^n$ ,  $g(T) = \sum_{n=0}^{\infty} b_n T^n \in R[[T]]$ , so that  $f(T) - g(T) = \sum_{n=0}^{\infty} (a_n - b_n) T^n$ . Let  $U$  be a subring of  $R$ . For  $d \in \mathbb{N}$ , we shall write

$$f(T) \equiv g(T) \pmod{U, \text{ degree } d} \Leftrightarrow a_n \equiv b_n \pmod{U} \text{ for all } 0 \leq n < d.$$

If this holds for all  $d \geq 1$  (so  $a_n - b_n \in U$  for all  $n \geq 0$ ), we shall simply write  $f(T) \equiv g(T) \pmod{U}$ . Finally if  $U = 0$ , we write  $f(T) \equiv g(T) \pmod{\text{degree } d}$ . Setting  $\bar{f}(T) = \sum_{n=0}^{d-1} a_n T^n \in R[T]$ , we have

$$f(T)^i \equiv \bar{f}(T)^i \pmod{\text{degree } d} \text{ for all } i \geq 1.$$

**Lemma 1.3.2** [Ha,1,2.4.2] *Let  $G(T) \in S[[T]]$  and let  $n = p^i m$ , where  $i \in \mathbb{N} \cup 0$  and  $m \in \mathbb{N}$ , then*

$$G(T)^{np} \equiv (G^\sigma(T^p))^n \pmod{p^{i+1}S}.$$

**Proof** Write  $G(T) = \sum_{n=0}^{\infty} a_n T^n$  then we have

$$G(T)^p \equiv \sum_{n=0}^{\infty} a_n^p T^{np} \pmod{pS}$$

(compare with the corresponding result for polynomials, and see the remarks preceding this lemma). By (FE1),  $\sigma(a_n) \equiv a_n^p \pmod{pS}$  for all  $n \geq 0$ , and so

$$G(T)^p \equiv G^\sigma(T^p) \pmod{pS}.$$

Now suppose  $i \geq 1$ , and assume by induction that  $G(T)^{p^i} \equiv (G^\sigma(T^p))^{p^{i-1}} \pmod{p^i S}$ . It follows that

$$G(T)^{p^{i+1}} = (G(T)^{p^i})^p \equiv (G^\sigma(T^p))^{p^i} \pmod{p^{i+1}S},$$

using the fact that  $(G^\sigma(T^p))^{p^{i-1}} \in S[[T]]$ . The result follows on raising both sides of the congruence to the  $m^{\text{th}}$  power.  $\square$

**Lemma 1.3.3** *Let  $G(T) \in R[[T]]_0$  and suppose the condition*

$$(*) \quad G(T) = rG^\sigma(T^p)$$

*holds. Then  $G(T)$  is identically zero.*

**Proof** Write  $G(T) = \sum_{n=1}^{\infty} a_n T^n$ , then  $(*)$  becomes

$$\sum_{n=1}^{\infty} a_n T^n = r \sum_{n=1}^{\infty} \sigma(a_n) T^{np},$$

from which it is clear that  $a_1 = 0$  (as  $np \geq 2$  for  $n \in \mathbb{N}$ ). Now take a fixed  $n \in \mathbb{N}$ . If  $p \nmid n$ , we must have  $a_n = 0$ , so assume  $p \mid n$ . Then  $a_n = r\sigma(a_{n/p})$ , and so induction gives  $a_n = 0$  in this case also. Therefore  $a_n = 0$  for all  $n \geq 1$ , as required.  $\square$

We can now prove the main result of this section.

**Theorem 1.3.4** (The Functional Equation Lemma) [Ha,1,2.4] *Let  $g(T) = \sum_{n=1}^{\infty} b_n T^n$  and  $\bar{g}(T) = \sum_{n=1}^{\infty} \bar{b}_n T^n \in S[[T]]_0$ , and suppose  $b_1$  is invertible in  $S$ . Define  $f_g(T)$  and  $f_{\bar{g}}(T)$  as in (16). Then the following hold:*

$$(i) \quad (f_g^{-1} \circ f_{\bar{g}})(T) \in S[[T]]_0.$$

$$(ii) \quad \text{If } h(T) = \sum_{n=1}^{\infty} c_n T^n \in S[[T]]_0, \text{ then there exists } \hat{h}(T) = \sum_{n=1}^{\infty} \hat{c}_n T^n \in S[[T]]_0 \text{ such that } (f_g \circ h)(T) = f_{\hat{h}}(T).$$

**Proof** (i) Write  $f_g(T) = \sum_{n=1}^{\infty} a_n T^n$  and  $f_{\bar{g}}(T) = \sum_{n=1}^{\infty} \bar{a}_n T^n$ . By (16) we have  $a_1 = b_1$ , which is invertible in  $S$  (and  $R$ ), and so  $f_g^{-1}$  exists. Set  $F(T) = (f_g^{-1} \circ f_{\bar{g}})(T) = \sum_{n=1}^{\infty} u_n T^n$ , where each  $u_n \in R$ . Since  $f_g^{-1}(T) \equiv a_1^{-1}T \pmod{\text{degree } 2}$ , we obtain

$$u_1 = a_1^{-1} \bar{a}_1 \in S,$$

as  $a_1 (= b_1)$  is invertible in  $S$ . Now let  $k \geq 2$ , and assume by induction that  $u_1, u_2, \dots, u_{k-1} \in S$ . We have, for all  $i \geq 1$ ,

$$\left( u_1 T + u_2 T^2 + \dots + u_{k-1} T^{k-1} \right)^i \equiv F(T)^i \pmod{\text{degree } k+i-1}.$$

In particular, for  $i \geq 2$ ,  $(u_1T + u_2T^2 + \cdots + u_{k-1}T^{k-1})^i \equiv F(T)^i \pmod{\text{degree } k+1}$ . For  $n \in \mathbb{N}$  we have  $np \geq 2$ , and so

$$(*_1) \quad F(T)^{np} \equiv G(T)^{np} \pmod{\text{degree } k+1},$$

where  $G(T) = \sum_{i=1}^{k-1} u_i T^i$ , for brevity. Now we have  $(F^\sigma(T^p))^n = (\sum_{i=1}^{\infty} \sigma(u_i) T^{ip})^n \equiv (\sum_{i=1}^{k-1} \sigma(u_i) T^{ip})^n \pmod{\text{degree } kp}$ , and  $kp \geq k+1$  (actually strict), which gives

$$(*_2) \quad (F^\sigma(T^p))^n \equiv (G^\sigma(T^p))^n \pmod{\text{degree } k+1}.$$

Write  $n = p^i m$ , where  $i \in \mathbb{N} \cup 0$  and  $m \in \mathbb{N}$  with  $(m, p) = 1$ . By assumption,  $G(T) \in S[[T]]_0$ , and so applying 1.3.2 to  $(*_1)$  and  $(*_2)$ , we obtain

$$(*_3) \quad F(T)^{np} \equiv (F^\sigma(T^p))^n \pmod{p^{i+1}S, \text{ degree } k+1}$$

(note that  $i$  depends on  $n$ ).

Now by (17),  $f_g(T) = g(T) + r f_g^\sigma(T^p)$ , where  $f_g(T) = \sum_{n=1}^{\infty} a_n T^n$ , and so

$$(*_4) \quad f_{\bar{g}}(T) = f_g(F(T)) = g(F(T)) + r \sum_{n=1}^{\infty} \sigma(a_n) F(T)^{np}.$$

By  $(*_3)$  we have  $r\sigma(a_n)F(T)^{np} \equiv r\sigma(a_n)(F^\sigma(T^p))^n \pmod{r\sigma(a_n)p^{i+1}S, \text{ degree } k+1}$ . Applying 1.3.1 we obtain

$$a_n p^i S \subseteq S \Rightarrow \sigma(a_n) p^i S \subseteq S,$$

since  $1 \in S$  and  $\sigma(S) \subseteq S$ . Therefore

$$r\sigma(a_n) p^{i+1} S = r p \sigma(a_n) p^i S \subseteq r p S \subseteq S,$$

by (FE2). Applying this to  $(*_4)$  we obtain

$$f_{\bar{g}}(T) \equiv g(F(T)) + r \sum_{n=1}^{\infty} \sigma(a_n) (F^\sigma(T^p))^n \pmod{S, \text{ degree } k+1}.$$

Now

$$\begin{aligned} \sum_{n=1}^{\infty} \sigma(a_n) (F^\sigma(T^p))^n &= f_g^\sigma(F^\sigma(T^p)) \\ &= (f_g^\sigma \circ F^\sigma)(T^p) \\ &= (f_g \circ F)^\sigma(T^p) \quad (\text{by (14)}) \\ &= f_{\bar{g}}^\sigma(T^p), \end{aligned}$$

and so

$$f_{\bar{g}}(T) \equiv g(F(T)) + r f_g^\sigma(T^p) \pmod{S, \text{ degree } k+1}.$$

By (17),  $f_{\bar{g}}(T) = \bar{g}(T) + r f_g^\sigma(T^p)$ , which gives

$$g(F(T)) \equiv \bar{g}(T) \equiv 0 \pmod{S, \text{ degree } k+1}.$$

By assumption  $F(T) \equiv u_k T^k \pmod{S, \text{ degree } k+1}$ , which together with the fact that  $g(T) \equiv b_1 T \pmod{\text{degree } 2}$ , gives

$$g(F(T)) \equiv b_1 u_k T^k \pmod{S, \text{ degree } k+1},$$

and so  $b_1 u_k T^k \equiv 0 \pmod{S, \text{ degree } k+1}$ . This means that  $b_1 u_k \in S$ , and so  $u_k \in S$  since  $b_1$  is invertible in  $S$ . This completes the proof of part (i) of 1.3.4.

(ii) Define two power series  $\hat{f}(T), \hat{h}(T) \in R[[T]]_0$  by

$$\hat{f}(T) = (f_g \circ h)(T) \text{ and } \hat{h}(T) = \hat{f}(T) - r \hat{f}^\sigma(T^p).$$

We first show that  $\hat{h}(T) \in S[[T]]_0$ :

$$\begin{aligned} \hat{f}(T) - r \hat{f}^\sigma(T^p) &= (f_g \circ h)(T) - r(f_g^\sigma \circ h^\sigma)(T^p) \quad (\text{using (14)}) \\ &= f_g(h(T)) - r \sum_{n=1}^{\infty} \sigma(a_n) (h^\sigma(T^p))^n \\ &\equiv f_g(h(T)) - r \sum_{n=1}^{\infty} \sigma(a_n) (h(T)^p)^n \quad (\text{since } h(T) \in S[[T]]) \\ &= f_g(h(T)) - r f_g^\sigma(h(T)^p) \\ &= g(h(T)) \quad (\text{by (17)}) \\ &\equiv 0, \end{aligned}$$

all congruences modulo  $S$ . To complete the proof we must show that  $G(T) = f_{\hat{h}}(T) - \hat{f}(T)$  satisfies condition (\*) of 1.3.3. Indeed  $G^\sigma(T) = f_{\hat{h}}^\sigma(T) - \hat{f}^\sigma(T)$  is clear, and so

$$\begin{aligned} r G^\sigma(T^p) &= r f_{\hat{h}}^\sigma(T^p) - r \hat{f}^\sigma(T^p) \\ &= f_{\hat{h}}(T) - \hat{h}(T) - r \hat{f}^\sigma(T^p) \quad (\text{by (17)}) \\ &= G(T), \end{aligned}$$

using the definition of  $\hat{h}(T)$ . This forces  $f_{\hat{h}}(T) = \hat{f}(T)$ . □

## 1.4 Applications

In this section we discuss some applications of the functional equation lemma to our studies. First we introduce two power series in  $\mathbb{Q}[[T]]$  which will play an important role in what follows:

$$l(T) = \log(1 + T) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n} T^n \quad \text{and} \quad \exp(T) = \sum_{n=0}^{\infty} \frac{T^n}{n!} .$$

It can be shown that

$$\exp(T) - 1 = l^{-1}(T) \tag{18}$$

(see [B1,IV,4.10] for more details). For a fixed prime  $p \in \mathbb{N}$ , we also define

$$e_p(T) = \exp \left( \sum_{i=0}^{\infty} \frac{T^{p^i}}{p^i} \right) \in \mathbb{Q}[[T]] .$$

We now consider the first of two applications of 1.3.4. The notation  $(R, S, \sigma, p, \text{ and } r)$  is as used in 1.3.

**Application 1:** Take  $R = \mathbb{Q}$ ,  $S = \mathbb{Z}_{(p)}$ ,  $\sigma = 1$ , and  $r = 1/p$ .

We must show that (FE1) is satisfied (it is clear that (FE2) holds). Let  $a \in \mathbb{Z}_{(p)}$  then  $a = x/y$ , where  $x, y \in \mathbb{Z}$  with  $y \neq 0$ , and  $(y, p) = 1$ . Then we have

$$\sigma(a) - a^p = a - a^p = \frac{x(y^{p-1} - x^{p-1})}{y^p} .$$

If  $p \mid x$  it is clear that  $a - a^p \in p\mathbb{Z}_{(p)}$ , so we may assume that  $p \nmid x$ . Then by Fermat's Little Theorem (see [Bu,5.3]), we have  $x^{p-1} \equiv 1 \pmod{p}$  and  $y^{p-1} \equiv 1 \pmod{p}$ , and so  $y^{p-1} - x^{p-1} \equiv 0 \pmod{p}$ . It follows that  $a - a^p \in p\mathbb{Z}_{(p)}$  as required.

Now define

$$g(T) = \begin{cases} \sum_{(n,2)=1} \frac{1}{n} (T^n - T^{2n}) & : p = 2 \\ \sum_{(n,p)=1} \frac{(-1)^{n+1}}{n} T^n & : p > 2 \end{cases} . \tag{19}$$

Also define  $\bar{g}(T) = T$ . Then we claim that

$$f_g(T) = l(T) \quad \text{and} \quad f_{\bar{g}}(T) = \sum_{i=0}^{\infty} \frac{T^{p^i}}{p^i} . \tag{20}$$

To see this, write  $g(T) = \sum_{n=1}^{\infty} b_n T^n$  and  $f_g(T) = \sum_{n=1}^{\infty} a_n T^n$ . First assume that  $p$  is *odd*. Let  $n = p^i m$  where  $i \in \mathbb{N} \cup 0$ , and  $m \in \mathbb{N}$  with  $(m, p) = 1$ . If  $i = 0$  (so  $(n, p) = 1$ ) then by (19),  $b_n = (-1)^{n+1}/n$ , and so (16) gives  $a_n = b_n = (-1)^{n+1}/n$ . Now suppose  $i \geq 1$ , so that  $(n, p) \neq 1$ , then (16) gives

$$a_n = b_n + \frac{1}{p} a_{n/p} = \frac{1}{p} a_{n/p} ,$$

since  $b_n = 0$  by (19). Now  $n/p = p^{i-1}m$ , so induction gives

$$a_{n/p} = \frac{(-1)^{n/p+1}}{n/p} .$$

Since  $n$  and  $n/p$  have the same parity, it follows that  $a_n = (-1)^{n+1}/n$ , as required. If  $p = 2$  then by (19),

$$b_n = \begin{cases} 1/n & : n \text{ odd} \\ -2/n & : n/2 \text{ odd} \\ 0 & : n/2 \text{ even} \end{cases} ,$$

and arguing as above yields the result in this case also (also see [Ha,1,2.1]). The expression for  $f_{\bar{g}}(T)$  is obtained similarly.

Now by (18), we have  $\exp(T) - 1 = f_g^{-1}(T)$ , and so  $(f_g^{-1} \circ f_{\bar{g}})(T) = e_p(T) - 1$ . Part (i) of 1.3.4 now implies that

$$e_p(T) \in \mathbb{Z}_{(p)}[[T]] .$$

We will now consider a generalization of this power series. Given  $d_i \in \mathbb{Q}$ ,  $i \geq 0$ , define

$$d(T) = \sum_{i=0}^{\infty} d_i T^{p^i} = d_0 T + d_1 T^p + d_2 T^{p^2} + \dots \in \mathbb{Q}[[T]] ,$$

and form the (composite) power series

$$\exp(d(T)) = \sum_{n=0}^{\infty} c_n T^n \in \mathbb{Q}[[T]] \tag{21}$$

(note that  $c_0 = 1$ ). An expression of the form (21) is known as an *Artin-Hasse exponential series*. We have the following

**Theorem 1.4.1** [Ha,1,2.3.3] *In (21) each  $c_n \in \mathbb{Z}_{(p)}$ ,  $n = 0, 1, 2, \dots$ , if and only if  $d_i = p^{-1}d_{i-1} + b_i$  for some  $b_i \in \mathbb{Z}_{(p)}$ , for all  $i = 0, 1, 2, \dots$  (where we take  $d_{-1} = 0$ ).*

**Proof** Suppose there are  $b_i \in \mathbb{Z}_{(p)}$  such that  $d_i = p^{-1}d_{i-1} + b_i$ ,  $i = 0, 1, 2, \dots$  (with  $d_{-1} = 0$ ). Define  $g(T)$  as in (19), and take  $\bar{g}(T) = \sum_{i=0}^{\infty} b_i T^{p^i}$ . Then we claim that

$$f_g(T) = l(T) \quad \text{and} \quad f_{\bar{g}}(T) = d(T).$$

The former was obtained in (20). To see the latter, write  $\bar{g}(T) = \sum_{n=1}^{\infty} \lambda_n T^n$  and  $f_{\bar{g}}(T) = \sum_{n=1}^{\infty} a_n T^n$ . Let  $n = p^i m$  where  $i \in \mathbb{N} \cup 0$ , and  $m \in \mathbb{N}$  with  $(m, p) = 1$ . Then

$$\lambda_n = \begin{cases} b_i & : m = 1 \\ 0 & : m > 1 \end{cases}.$$

If  $m > 1$ , we can use (16), and induction on  $i$ , to conclude that  $a_n = 0$ . Now suppose  $m = 1$  (so that  $n = p^i$ ). For  $i = 0$  we have, by (16),  $a_1 = b_0 = d_0$ . If  $i \geq 1$  then (16) gives

$$a_n = \frac{1}{p} a_{n/p} + b_i.$$

Since  $n/p = p^{i-1}$ , induction gives  $a_{n/p} = d_{i-1}$ , from which  $a_n = d_i$ , as required. (Note that (20) is a special case of this with  $b_0 = d_0 = 1$  and  $b_i = 0$  for  $i \geq 1$ .) Now (18) gives  $\exp(T) - 1 = f_g^{-1}(T)$ , and so  $(f_g^{-1} \circ f_{\bar{g}})(T) = \exp(d(T)) - 1$ . Part (i) of 1.3.4 now implies that  $c_n \in \mathbb{Z}_{(p)}$  for all  $n \geq 0$ .

Conversely suppose  $c_n \in \mathbb{Z}_{(p)}$  for all  $n \geq 0$ . Write  $h(T) = \exp(d(T)) - 1 = \sum_{n=1}^{\infty} c_n T^n \in \mathbb{Z}_{(p)}[[T]]_0$ . Then by part (ii) of 1.3.4 there exists  $\hat{h}(T) = \sum_{n=1}^{\infty} \hat{c}_n T^n \in \mathbb{Z}_{(p)}[[T]]_0$  such that  $(f_g \circ h)(T) = f_{\hat{h}}(T)$ . Using (18) we obtain

$$(f_g \circ h)(T) = l(\exp(d(T)) - 1) = d(T);$$

that is,

$$f_{\hat{h}}(T) = \sum_{i=0}^{\infty} d_i T^{p^i}.$$

Write  $n = p^i m$  where  $i \in \mathbb{N} \cup 0$ , and  $m \in \mathbb{N}$  with  $(m, p) = 1$ . Consider the case where  $m = 1$ ; that is, when  $n = p^i$ . By (16) we have

$$d_0 = \hat{c}_1 \quad \text{and} \quad d_i = \frac{1}{p} d_{i-1} + \hat{c}_{p^i}, \quad i \geq 1.$$

(Note that when  $m > 1$ , (16) gives  $\hat{c}_n = 0$ .) Define  $b_i = \hat{c}_{p^i}$  for  $i \geq 0$ . Then, on taking  $d_{-1} = 0$ , we obtain

$$d_i = \frac{1}{p} d_{i-1} + b_i, \quad \text{for all } i \geq 0,$$



where each  $b_i \in \mathbb{Z}_{(p)}$ , as required.  $\square$

The next application of 1.3.4 is a generalization of Application 1.

**Application 2:** Take  $R = \mathbb{Q}[X] = \mathbb{Q}[X_0, X_1, X_2, \dots]$ ,  $S = \mathbb{Z}_{(p)}[X]$ , and  $r = 1/p$ . Let  $\sigma : R \rightarrow R$  be the (unital) ring homomorphism, where

$$\sigma(q) = q, \quad q \in \mathbb{Q} \quad \text{and} \quad \sigma(X_i) = X_i^p, \quad i \geq 0.$$

We claim that

$$(*) \quad \sigma(a) \equiv a^p \pmod{pS} \quad \text{for all } a \in S.$$

To see this, first consider  $a = \lambda X_{i_1}^{t_1} \cdots X_{i_n}^{t_n}$ , where  $\lambda \in \mathbb{Z}_{(p)}$  and  $i_m, t_m \in \mathbb{N} \cup 0$ ,  $1 \leq m \leq n$ . Since  $\lambda \equiv \lambda^p \pmod{p\mathbb{Z}_{(p)}}$  for all  $\lambda \in \mathbb{Z}_{(p)}$  (see Application 1), it follows that  $(*)$  holds for this  $a$ . Taking finite sums of such elements, and using the fact that  $(a + b)^p \equiv a^p + b^p \pmod{pS}$  for  $a, b \in S$ , we obtain  $(*)$  for all elements  $a \in S$ . Therefore conditions (FE1) and (FE2) are satisfied (condition (FE2) being trivial). Note that  $\sigma = 1$ , as used in Application 1, does *not* satisfy condition (FE1): for example,  $X_0 - X_0^p \notin pS$ .

Given  $d_i \in \mathbb{Q}[X]$ ,  $i \geq 0$ , define

$$d(T) = \sum_{i=0}^{\infty} d_i T^{p^i} = d_0 T + d_1 T^p + d_2 T^{p^2} + \cdots \in \mathbb{Q}[X][[T]],$$

then we can form the (composite) power series

$$\exp(d(T)) = \sum_{n=0}^{\infty} c_n T^n \in \mathbb{Q}[X][[T]]. \quad (22)$$

We have the following

**Theorem 1.4.2** *In (22) each  $c_n \in \mathbb{Z}_{(p)}[X]$ ,  $n = 0, 1, 2, \dots$ , if and only if  $d_i = p^{-1}\sigma(d_{i-1}) + b_i$  for some  $b_i \in \mathbb{Z}_{(p)}[X]$ , for all  $i = 0, 1, 2, \dots$  (where we take  $d_{-1} = 0$ ).*

**Proof** Suppose there are  $b_i \in \mathbb{Z}_{(p)}[X]$  such that  $d_i = p^{-1}\sigma(d_{i-1}) + b_i$ ,  $i = 0, 1, 2, \dots$  (with  $d_{-1} = 0$ ). Define  $g(T)$  as in (19) (its coefficients are in  $\mathbb{Z}_{(p)} \subseteq \mathbb{Z}_{(p)}[X]$ ), and take  $\bar{g}(T) = \sum_{i=0}^{\infty} b_i T^{p^i}$ . Then we claim that

$$f_g(T) = l(T) \quad \text{and} \quad f_{\bar{g}}(T) = d(T).$$

For the former, write  $f_g(T) = \sum_{n=1}^{\infty} a_n T^n$ , and let  $n = p^i m$ , where  $i \in \mathbb{N} \cup 0$ , and  $m \in \mathbb{N}$  with  $(m, p) = 1$ . Using (16) and induction on  $i$ , we obtain  $a_n \in \mathbb{Q}$  for all  $n \geq 1$  (and so  $\sigma(a_n) = a_n$  for all  $n \geq 1$ ). This gives  $f_g(T) = l(T)$  as in (20). To see the latter, write  $f_{\bar{g}}(T) = \sum_{n=1}^{\infty} \bar{a}_n T^n$ . Again let  $n = p^i m$  where  $i \in \mathbb{N} \cup 0$ , and  $m \in \mathbb{N}$  with  $(m, p) = 1$ . Arguing as in the proof of 1.4.1, we obtain

$$\bar{a}_n = \begin{cases} d_i & : m = 1 \\ 0 & : m > 1 \end{cases},$$

as required. The rest of the proof (including the converse argument) is practically the same as that in 1.4.1.  $\square$

**Special Case** We now consider an important special case of 1.4.2, which will be needed in the subsequent sections. Refer to the above for notation. Keep  $p$  arbitrary, and take

$$b_i = X_i \text{ for all } i \geq 0,$$

which is the most natural non-trivial case. Then define  $d_{-1} = 0$ , and

$$(**) \quad d_i = \frac{1}{p} \sigma(d_{i-1}) + b_i = \frac{1}{p} \sigma(d_{i-1}) + X_i \text{ for } i \geq 0.$$

To emphasize the role of  $X = (X_i) \in W(A)$ , where  $A$  is given on p.6, we now introduce the following notation: Let  $i \geq 0$ , and define

$$d(X)_i = d_i \text{ and } c(X)_i = c_i,$$

where the  $c_i$ ,  $i \geq 0$ , are defined by (22). Using induction on  $(**)$  we obtain

$$d(X)_0 = X_0 \text{ and } d(X)_i = \frac{1}{p^i} X_0^{p^i} + \frac{1}{p^{i-1}} X_1^{p^{i-1}} + \cdots + \frac{1}{p} X_{i-1}^p + X_i, \quad i \geq 1. \quad (23)$$

Now write  $d(X, T) = d(T)$ , so that

$$d(X, T) = \sum_{i=0}^{\infty} d(X)_i T^{p^i}.$$

Then it follows from 1.4.2 that

$$\exp(d(X, T)) = \sum_{i=0}^{\infty} c(X)_i T^i \in \mathbb{Z}_{(p)}[X][[T]].$$

Note that  $c(X)_i = X_0^i / i!$ , for  $0 \leq i \leq p-1$ .

For future reference, we include the following (refer to the above for notation):

**Lemma 1.4.3** *Let  $j \geq 1$  and suppose  $1 \leq i < p^j$ . Then the following hold:*

- (i)  $c(X)_0 = 1$  and  $c(X)_1 = X_0$ .
- (ii)  $c(X)_i \in \mathbb{Z}_{(p)}[X_0, X_1, \dots, X_{j-1}]_0$ .
- (iii)  $c(X)_{p^j} - X_j \in \mathbb{Z}_{(p)}[X_0, X_1, \dots, X_{j-1}]_0$ .

**Proof** We have

$$(*_1) \quad \exp(d(X)_0 T + d(X)_1 T^p + \dots + d(X)_{j-1} T^{p^{j-1}} + d(X)_j T^{p^j} + \dots) = \sum_{i=0}^{\infty} c(X)_i T^i,$$

where by 1.4.2,

$$(*_2) \quad c(X)_i \in \mathbb{Z}_{(p)}[X] \text{ for } i \geq 0.$$

(Also recall that  $\exp(T) = \sum_{n=0}^{\infty} T^n/n!$ .) Equating coefficients of  $T^0$  and  $T^1$  in  $(*_1)$ , gives  $c(X)_0 = 1$  and  $c(X)_1 = d(X)_0 = X_0$ , respectively (see (23)). This proves part (i). Now by (23),

$$(*_3) \quad d(X)_k \in \mathbb{Q}[X_0, X_1, \dots, X_{j-1}]_0, \quad 0 \leq k \leq j-1.$$

By  $(*_1)$  we obtain  $c(X)_i = Q_i(d(X)_0, d(X)_1, \dots, d(X)_{j-1})$ , for some  $Q_i \in \mathbb{Q}[Y_0, Y_1, \dots, Y_{j-1}]_0$ . Part (ii) follows from this, using  $(*_2)$  and  $(*_3)$ . It remains to prove part (iii). Equating coefficients of  $T^{p^j}$  in  $(*_1)$  gives

$$c(X)_{p^j} - d(X)_j = R_j(d(X)_0, d(X)_1, \dots, d(X)_{j-1}),$$

for some  $R_j \in \mathbb{Q}[Y_0, Y_1, \dots, Y_{j-1}]_0$ . Now by (23),

$$d(X)_j - X_j \in \mathbb{Q}[X_0, X_1, \dots, X_{j-1}]_0.$$

The result follows using  $(*_2)$  and  $(*_3)$ . □

## 1.5 Witt Groups and Artin-Hasse Exponentials

In this section we explain how the Artin-Hasse exponential series are related to the Witt vectors introduced in section 1. Throughout  $p$  denotes a fixed prime in  $\mathbb{N}$ ,  $A = \mathbb{Q}[X_i, Y_j]$ , and  $B = \mathbb{Z}_{(p)}[X_i, Y_j]$ ,  $i, j = 0, 1, 2, \dots$ .

In (23) we defined, for  $X = (X_i) \in W(A)$ ,

$$d(X)_0 = X_0 \text{ and } d(X)_i = \frac{1}{p^i} X_0^{p^i} + \frac{1}{p^{i-1}} X_1^{p^{i-1}} + \dots + \frac{1}{p} X_{i-1}^p + X_i, \quad i \geq 1,$$

and also

$$d(X, T) = \sum_{i=0}^{\infty} d(X)_i T^{p^i}.$$

Exponentiating this gives

$$\exp(d(X, T)) = \sum_{i=0}^{\infty} c(X)_i T^i,$$

where by 1.4.2,

$$c(X)_i \in \mathbb{Z}_{(p)}[X] = \mathbb{Z}_{(p)}[X_0, X_1, X_2, \dots].$$

This property allows us to construct an analogous power series in  $R[[T]]$ , where  $R$  is an arbitrary commutative ring with identity,  $1 \in R$ , of characteristic  $p$ . Let  $\bar{c}(X)_i$  be the polynomial in  $R[X]$  obtained from  $c(X)_i$ , by replacing each coefficient  $t \in \mathbb{Z}_{(p)}$  by  $\bar{t} \in R$ , where  $\bar{t}$  is the image of  $t$  under the natural homomorphism  $\mathbb{Z}_{(p)} \rightarrow R$  (which sends  $a/b$  to  $(a \cdot 1)(b \cdot 1)^{-1}$ , where  $a \in \mathbb{Z}$ ,  $b \in \mathbb{Z} - 0$  with  $(b, p) = 1$ ). Let  $x = (x_i) \in W(R)$ . Substituting  $x$  for  $X$  in  $\bar{c}(X)_i$  gives  $\bar{c}(x)_i \in R$ . Now define

$$e_p(T, x) = \sum_{i=0}^{\infty} \bar{c}(x)_i T^i \in R[[T]]. \quad (24)$$

Note the similarities between this construction, and that of the Witt rings  $W(R)$  and  $W_n(R)$ ,  $n \geq 1$ , of section 1. We shall call (24) the *Artin-Hasse exponential of  $x$* .

Before proving the main result (1.5.3) of this section, we need a couple of basic lemmas. The following property will also be required: Fix  $a = (a_i) \in W(A)$ . Given  $q(X) \in \mathbb{Q}[X] = \mathbb{Q}[X_0, X_1, X_2, \dots]$ , we can substitute  $a_i$  for  $X_i$ ,  $i \geq 0$ , to obtain an element  $q(a) \in A$ . Let  $\sigma : \mathbb{Q}[X] \rightarrow A$  denote the resulting (unital) ring homomorphism. For  $f(T) = \sum_{i=0}^{\infty} \lambda_i T^i \in \mathbb{Q}[X][[T]]$ , define  $f^\sigma(T) = \sum_{i=0}^{\infty} \sigma(\lambda_i) T^i \in A[[T]]$ . Then for  $g(T) \in \mathbb{Q}[X][[T]]_0$ , we have

$$(f^\sigma \circ g^\sigma)(T) = (f \circ g)^\sigma(T)$$

(compare with (14)). Take  $f(T) = \exp(T)$  and  $g(T) = d(X, T)$ , and write  $d(a, T) = g^\sigma(T) = \sum_{i=0}^{\infty} d(a)_i T^{p^i}$ . Then

$$\exp(d(a, T)) = \sum_{i=0}^{\infty} c(a)_i T^i. \quad (25)$$

We now come to the first of our two lemmas (refer to the above for notation).

**Lemma 1.5.1** *Let  $a = (a_i) \in W(A)$ . Then*

$$d(a)_i = \frac{1}{p^i} a^{(i)}, \quad i \geq 0,$$

where  $a^{(i)}$ ,  $i \geq 0$ , is defined in (2).

**Proof** This follows immediately from the definitions (2) and (23). □

Next we have

**Lemma 1.5.2** *Take  $X = (X_i)$ ,  $Y = (Y_i) \in W(A)$ . Then*

$$d(X + Y, T) = d(X, T) + d(Y, T),$$

where  $X + Y$  denotes addition of Witt vectors.

**Proof** By (2) and (4), we have  $X + Y = [X^{(i)} + Y^{(i)}] = ((X + Y)_i)$ , where

$$X^{(0)} + Y^{(0)} = (X + Y)_0,$$

$$X^{(i)} + Y^{(i)} = (X + Y)_0^{p^i} + p(X + Y)_1^{p^{i-1}} + \cdots + p^{i-1}(X + Y)_{i-1}^{p^1} + p^i(X + Y)_i, \quad i \geq 1.$$

It follows from (23) that

$$d(X + Y)_i = \frac{1}{p^i} X^{(i)} + \frac{1}{p^i} Y^{(i)}, \quad i \geq 0.$$

That is, by 1.5.1,

$$(*) \quad d(X + Y)_i = d(X)_i + d(Y)_i, \quad i \geq 0.$$

Therefore

$$\begin{aligned}
d(X + Y, T) &= \sum_{i=0}^{\infty} d(X + Y)_i T^{p^i} \\
&= \sum_{i=0}^{\infty} (d(X)_i + d(Y)_i) T^{p^i} \quad (\text{by } (*)) \\
&= \sum_{i=0}^{\infty} d(X)_i T^{p^i} + \sum_{i=0}^{\infty} d(Y)_i T^{p^i} \\
&= d(X, T) + d(Y, T),
\end{aligned}$$

as required. □

We can now prove the main result of this section.

**Theorem 1.5.3** *Let  $R$  be a commutative ring with identity,  $1 \in R$ , of characteristic  $p$ . Then the map*

$$\begin{aligned}
\phi : W(R) &\rightarrow R[[T]] \\
x &\mapsto e_p(T, x)
\end{aligned}
,$$

*satisfies  $\phi(x + y) = \phi(x)\phi(y)$ , for all  $x, y \in W(R)$ , where  $x + y$  denotes addition of Witt vectors, and  $e_p(T, x)$  is defined in (24).*

**Proof** Let  $x = (x_i)$ ,  $y = (y_i)$  be two fixed elements of  $W(R)$ . Write  $B = \mathbb{Z}_{(p)}[X_i, Y_j]$ ,  $i, j = 0, 1, 2, \dots$ , as on p.36. Then define a map  $\sigma : B \rightarrow R$  by

$$\sigma(a/b) = (a \cdot 1)(b \cdot 1)^{-1}, \quad \sigma(X_i) = x_i, \quad \text{and} \quad \sigma(Y_i) = y_i,$$

where  $a \in \mathbb{Z}$ ,  $b \in \mathbb{Z} - 0$  with  $(b, p) = 1$ , and extend this to a homomorphism of rings. For  $f(T) = \sum_{i=0}^{\infty} a_i T^i \in B[[T]]$ , define (as usual)  $f^\sigma(T) = \sum_{i=0}^{\infty} \sigma(a_i) T^i \in R[[T]]$ . This determines a ring homomorphism

$$\begin{aligned}
\theta = \sigma_{[[T]]} : B[[T]] &\rightarrow R[[T]] \\
f(T) &\mapsto f^\sigma(T)
\end{aligned}
.$$

To see this, note that by definition,

$$\left( \sum_{i=0}^{\infty} a_i T^i \right) \left( \sum_{j=0}^{\infty} b_j T^j \right) = \sum_{k=0}^{\infty} \left( \sum_{i+j=k} a_i b_j \right) T^k,$$

where each  $a_i, b_j \in B$ . Since  $\sigma$  is a ring homomorphism, it follows that  $\theta$  is *multiplicative* (the rest is clear).

Now for  $X = (X_i)$ ,  $Y = (Y_i) \in W(A)$ , we have by 1.5.2,

$$\exp(d(X + Y, T)) = \exp(d(X, T) + d(Y, T)) = \exp(d(X, T)) \exp(d(Y, T))$$

(for the latter equality, see [B1,IV,4.10] and [ZS,VII,1,(9)]). Using (25) we obtain

$$(**) \quad \sum_{i=0}^{\infty} c(X + Y)_i T^i = \left( \sum_{i=0}^{\infty} c(X)_i T^i \right) \left( \sum_{i=0}^{\infty} c(Y)_i T^i \right).$$

Now for  $i \geq 0$ , we have

$$\sigma(c(X)_i) = \bar{c}(x)_i, \quad \sigma(c(Y)_i) = \bar{c}(y)_i, \quad \text{and} \quad \sigma(c(X + Y)_i) = \bar{c}(x + y)_i.$$

For the latter equality, it suffices to note that, by (10) and (12),

$$(x + y)_j = \bar{A}_j(x_r, y_s) = \sigma(A_j(X_r, Y_s)) = \sigma((X + Y)_j), \quad j \geq 0, \quad 0 \leq r, s \leq j.$$

Applying  $\theta$  to (\*\*) gives, since  $\theta$  is multiplicative,

$$(***) \quad \sum_{i=0}^{\infty} \bar{c}(x + y)_i T^i = \left( \sum_{i=0}^{\infty} \bar{c}(x)_i T^i \right) \left( \sum_{i=0}^{\infty} \bar{c}(y)_i T^i \right).$$

Therefore

$$\begin{aligned} \phi(x + y) &= e_p(T, x + y) \\ &= \sum_{i=0}^{\infty} \bar{c}(x + y)_i T^i \quad (\text{by definition (24)}) \\ &= \left( \sum_{i=0}^{\infty} \bar{c}(x)_i T^i \right) \left( \sum_{i=0}^{\infty} \bar{c}(y)_i T^i \right) \quad (\text{by (***)}) \\ &= e_p(T, x) e_p(T, y) \quad (\text{by definition (24)}) \\ &= \phi(x) \phi(y), \end{aligned}$$

as required. □

For an alternative proof of 1.5.3, consult [Ha,III,17.4.23].

## 1.6 Artin-Hasse Exponentials of Nilpotent Matrices

Let  $R$  be a commutative ring with identity,  $1 \in R$ , of characteristic  $p$ , with  $p$  a fixed prime in  $\mathbb{N}$ . In section 5 we defined a multiplicative map from  $W(R)$  to  $R[[T]]$ , sending  $x \in W(R)$  to its Artin-Hasse exponential,  $e_p(T, x)$ . We now obtain a ‘matrix version’ of this result, by evaluating  $e_p(T, x)$  at a *nilpotent* matrix.

The following notation will be required: Let  $S$  be an *arbitrary* commutative ring (with identity). Let  $0 \neq N \in M(n, S)$ ,  $n \geq 1$ , be nilpotent. Fix a prime  $p \in \mathbb{N}$ . Then there exists  $t \in \mathbb{N}$  with

$$N^{p^t} = 0 \quad \text{and} \quad N^{p^i} \neq 0, \quad 0 \leq i < t.$$

We shall call  $t$  the *p-nilpotency* of  $N$ , and write  $p\text{-nilp}(N) = t$ . The matrix  $N$  may of course be zero before the  $(p^t)$ -th power.

Now let  $0 \neq N \in M(n, R)$ ,  $n \geq 1$ , be nilpotent. Then  $p\text{-nilp}(N) = t$ , for some  $t \in \mathbb{N}$ . Given  $f(T) = \sum_{i=0}^{\infty} a_i T^i \in R[[T]]$ , we can substitute  $N$  for  $T$  to obtain a matrix  $f(N) = \sum_{i=0}^{p^t-1} a_i N^i \in M(n, R)$ , where  $N^0$  is defined to be  $I_n$ . This determines a ring homomorphism

$$\begin{aligned} \psi : R[[T]] &\rightarrow M(n, R) \\ f(T) &\mapsto f(N) \end{aligned}.$$

For multiplication, note that

$$\left( \sum_{i=0}^{p^t-1} a_i N^i \right) \left( \sum_{j=0}^{p^t-1} b_j N^j \right) = \sum_{k=0}^{2(p^t-1)} \left( \sum_{i+j=k} a_i b_j \right) N^k = \sum_{k=0}^{p^t-1} \left( \sum_{i+j=k} a_i b_j \right) N^k,$$

since  $N^{p^t} = 0$ . The rest is clear. Note that  $\psi$  is not injective.

Let  $y = (y_0, y_1, \dots, y_{t-1}) \in W_t(R)$ , and define  $x = (x_i) \in W(R)$  by

$$x_i = \begin{cases} y_i & : 0 \leq i \leq t-1 \\ \text{arbitrary} & : i \geq t \end{cases}. \quad (26)$$

We shall call  $x$  an *extension* of  $y$ . Recall from (24) that the Artin-Hasse exponential of  $x$  is given by

$$e_p(T, x) = \sum_{i=0}^{\infty} \bar{c}(x)_i T^i \in R[[T]].$$



With this in mind, we shall define

$$e_p(N, y) = \psi(e_p(T, x)) = \sum_{i=0}^{p^t-1} \bar{c}(x)_i N^i \in M(n, R). \quad (27)$$

We now show that (27) is *independent* of the chosen extension of  $y$ . Write  $A = \mathbb{Q}[X] = \mathbb{Q}[X_0, X_1, X_2, \dots]$ , and take  $X = (X_i) \in W(A)$ . By 1.4.3(i) and (ii), we have

$$c(X)_i \in \mathbb{Z}_{(p)}[X_0, X_1, \dots, X_{j-1}], \quad j \geq 1, \quad 0 \leq i < p^j$$

(we are not assuming  $j$  is the least such integer). In particular, for  $j = t$ , we obtain

$$\bar{c}(X)_i = P_i(X_0, X_1, \dots, X_{t-1}) \in R[X_0, X_1, \dots, X_{t-1}], \quad 0 \leq i < p^t.$$

Substituting  $x$  for  $X$  gives, by (26),

$$\bar{c}(x)_i = P_i(y_0, y_1, \dots, y_{t-1}), \quad 0 \leq i < p^t. \quad (28)$$

Since  $N^{p^t} = 0$ , it follows from (28) that  $e_p(N, y)$  is independent of the extension of  $y$ , as required. This permits us to write  $\bar{c}(y)_i = \bar{c}(x)_i$  for  $0 \leq i < p^t$ . The matrix  $e_p(N, y)$  in (27) will be called the *Artin-Hasse exponential of  $N$  with respect to  $y$* .

We have the following analogue of 1.5.3 (where  $p$  is a fixed prime in  $\mathbb{N}$ ):

**Theorem 1.6.1** *Let  $R$  be a commutative ring with identity,  $1 \in R$ , of characteristic  $p$ . Suppose  $0 \neq N \in M(n, R)$ ,  $n \geq 1$ , is nilpotent, with  $p\text{-nilp}(N) = t \in \mathbb{N}$ . Then the map*

$$\begin{aligned} \phi : W_t(R) &\rightarrow M(n, R) \\ y &\mapsto e_p(N, y) \end{aligned},$$

*satisfies  $\phi(y + y') = \phi(y)\phi(y')$  for all  $y, y' \in W_t(R)$ , where  $y + y'$  denotes addition of Witt vectors, and  $e_p(N, y)$  is defined in (27).*

**Proof** Let  $y = (y_0, y_1, \dots, y_{t-1})$ ,  $y' = (y'_0, y'_1, \dots, y'_{t-1}) \in W_t(R)$ , and let  $x = (x_i)$ ,  $x' = (x'_i) \in W(R)$  be (arbitrary) extensions of  $y$  and  $y'$ , respectively. It follows from definition (12) of addition in  $W_t(R)$  and  $W(R)$ , and (26), that

$$(x + x')_i = (y + y')_i, \quad 0 \leq i \leq t-1.$$

That is,  $x + x'$  is an extension of  $y + y'$ . Now by 1.5.3, we have

$$(*) \quad e_p(T, x) e_p(T, x') = e_p(T, x + x').$$

Now let  $\psi : R[[T]] \rightarrow M(n, R)$  be the ring homomorphism defined above, where  $f(T) \xrightarrow{\psi} f(N)$ . Applying  $\psi$  to  $(*)$  we obtain, by definition (27),

$$e_p(N, y) e_p(N, y') = e_p(N, y + y'),$$

as required. □

We now consider the case where  $R = K$ , an algebraically closed field of characteristic  $p > 0$ . For  $n \geq 1$ , we define

$$\begin{aligned} u(n, K) &= \{(a_{ij}) \in M(n, K) : a_{ij} = 0, i \geq j\} \\ U(n, K) &= \{(a_{ij}) \in M(n, K) : a_{ij} = 0, i > j \text{ and } a_{ii} = 1\} \end{aligned}$$

That is,  $u(n, K)$  is the set of all *strictly upper triangular* matrices over  $K$  (a subring of  $M(n, K)$ ), and  $U(n, K)$  is the set of all *uni-upper triangular* matrices over  $K$  (a subgroup of  $SL(n, K)$ ).

Now fix  $0 \neq N \in u(n, K)$ ,  $n \geq 2$ . Since  $N$  is nilpotent (see 1.6.2(ii) to follow), we have  $p\text{-nilp}(N) = t$ , for some  $t \in \mathbb{N}$ . Then for each  $y = (y_0, y_1, \dots, y_{t-1}) \in W_t(K)$ , we have (see (27))

$$e_p(N, y) = \sum_{i=0}^{p^t-1} \bar{c}(y)_i N^i \in U(n, K) \subseteq SL(n, K)$$

(where  $\bar{c}(y)_0 = 1 \in K$  by 1.4.3(i)). Now, by 1.4.3(ii), we have  $\bar{c}(X)_i \in K[X_0, X_1, \dots, X_{t-1}]$ , where  $0 \leq i < p^t$ , and so each ‘coordinate’ of  $e_p(N, y)$  is of the form  $q(y)$ , for some  $q(X) \in K[X_0, X_1, \dots, X_{t-1}]$ , independent of  $y$ . It then follows from 1.6.1 that the map

$$\begin{aligned} \phi : W_t(K) &\rightarrow SL(n, K) \\ y &\mapsto e_p(N, y) \end{aligned} \tag{29}$$

is a *morphism of algebraic groups*. It will be shown shortly that  $\phi$  is in fact an *isomorphism* of algebraic groups onto its image (1.6.4).

First it will be convenient to introduce the following notation: Let  $e_{ij}$ ,  $1 \leq i, j \leq n$ , denote the  $n \times n$  matrix over  $K$ , or any commutative ring with identity, with  $(i, j)$ -th coefficient 1,

and all other coefficients equal to 0. These *elementary matrices* multiply together as follows:

$$e_{ij} e_{kl} = \delta_{jk} e_{il}, \quad \text{where} \quad \delta_{jk} = \begin{cases} 1 & : j = k \\ 0 & : j \neq k \end{cases} ; \quad 1 \leq i, j, k, l \leq n.$$

Now suppose  $1 \leq i < j \leq n$ , and define

$$\text{ht}(e_{ij}) = j - i,$$

so that  $1 \leq \text{ht}(e_{ij}) \leq n - 1$ . Given  $0 \neq N \in u(n, K)$ ,  $n \geq 2$ , we can write

$$N = \sum_{1 \leq i < j \leq n} \lambda_{ij} e_{ij}, \quad \text{each } \lambda_{ij} \in K.$$

Now define

$$\text{ht}(N) = \min\{\text{ht}(e_{ij}) : 1 \leq i < j \leq n \text{ and } \lambda_{ij} \neq 0\},$$

so that  $1 \leq \text{ht}(N) \leq n - 1$ . If  $N = e_{ij}$  the two definitions coincide. For  $N = 0$  we shall define  $\text{ht}(N) = n$ . We shall also say that  $\lambda_{ij}$ ,  $1 \leq i < j \leq n$ , is a height  $j - i$  element of  $N$ . Next define, for  $1 \leq r \leq n - 1$ ,

$$H(r) = \{N \in u(n, K) : \text{ht}(N) \geq r\},$$

and for  $r \geq n$ , define  $H(r) = 0$ . It is then clear that

$$u(n, K) = H(1) \supsetneq H(2) \supsetneq \cdots \supsetneq H(n-1) \supsetneq H(n) = 0.$$

For  $r, s \in \mathbb{N}$ , let  $H(r)H(s)$  denote the set of all finite sums of products  $N_r N_s$ , where  $N_r \in H(r)$ ,  $N_s \in H(s)$ .

We now have the following well-known result:

**Lemma 1.6.2** [HT] *Let  $r, s \in \mathbb{N}$ , then the following hold:*

$$(i) \quad H(r)H(s) \subseteq H(r+s).$$

(ii) *If  $N \in H(r)$  then  $N^i \in H(ir)$ ,  $i \geq 1$ . In particular,  $N$  is nilpotent.*

**Proof** It suffices to prove part (i), with part (ii) following by induction. We first show that the result is true for the product of  $e_{ij} \in H(r)$  and  $e_{kl} \in H(s)$ . If  $j \neq k$  then  $e_{ij}e_{kl} = 0 \in H(r+s)$ , so assume  $j = k$ . Then  $e_{ij}e_{kl} = e_{il}$ . Now by choice,

$$j - i \geq r \text{ and } l - j \geq s \Rightarrow l - i \geq r + s.$$

Therefore  $e_{il} \in H(r + s)$ , as required. The result follows in general from the fact that every  $N \in H(r)$  is a linear combination of elements of the set  $\{e_{ij} : j - i \geq r\}$ .  $\square$

Note that 1.6.2 holds for *any* commutative ring with identity. Before returning to the map  $\phi$  of (29), we require the following technical lemma concerning the ‘coordinates’ of the matrix  $e_p(N, y)$ . We shall write  $K[T] = K[T_{ij}]$ ,  $1 \leq i, j \leq n$ , for the coordinate ring of the variety  $M(n, K) = K^{n^2}$ .

**Lemma 1.6.3** *Let  $K$  be a field of characteristic  $p > 0$ . Take  $0 \neq N \in u(n, K)$ ,  $n \geq 2$ , and suppose  $p\text{-nilp}(N) = t \in \mathbb{N}$ . Then there exists fixed polynomials  $q_k(T) \in K[T] = K[T_{ij}]$ ,  $1 \leq i, j \leq n$ ,  $0 \leq k \leq t - 1$ , satisfying the following property: Let  $y = (y_0, y_1, \dots, y_{t-1}) \in W_t(K)$  be arbitrary, and write  $a = e_p(N, y)$ . Then*

$$y_k = q_k(a), \quad 0 \leq k \leq t - 1.$$

**Proof** Suppose  $e \in \mathbb{N}$  satisfies  $N^e = 0$ , whilst  $N^i \neq 0$ ,  $1 \leq i < e$  (note that  $p^{t-1} < e \leq p^t$ ). Write

$$(*_1) \quad (a_{ij}(X)) = \sum_{i=0}^{e-1} \bar{c}(X)_i N^i \in M(n, K[X_0, X_1, \dots, X_{t-1}])$$

(where  $1 \leq i, j \leq n$ ; see 1.4.3(ii)). By 1.6.2(i), we have

$$(*_2) \quad 1 \leq \text{ht}(N) < \text{ht}(N^2) < \text{ht}(N^3) < \dots < \text{ht}(N^e) = n.$$

Let  $y = (y_0, y_1, \dots, y_{t-1}) \in W_t(K)$  be arbitrary, and write  $a_{ij} = a_{ij}(y)$ ,  $1 \leq i, j \leq n$ . Then  $a = (a_{ij}) = e_p(N, y)$  by definition (27). Suppose  $N = (b_{ij})$ ,  $1 \leq i, j \leq n$ , and that  $\text{ht}(N) = r$ , where  $1 \leq r \leq n - 1$ . Let  $b = b_{ij}$  be a *non-zero* coordinate of  $N$  of height  $j - i = r$ . Now by 1.4.3(i), we have  $\bar{c}(X)_1 = X_0$  (and so  $\bar{c}(y)_1 = y_0$ ). Using  $(*_1)$  and  $(*_2)$ , we obtain

$$bX_0 = a_{ij}(X) \Rightarrow X_0 = b^{-1}a_{ij}(X).$$

Define  $q_0(T) = b^{-1}T_{ij} \in K[T]$ , then  $q_0(a) = b^{-1}a_{ij} = y_0$ , and so the lemma holds for  $k = 0$ . Now let  $t \geq 2$ ,  $1 \leq k \leq t - 1$ , and assume by induction that there exists fixed polynomials  $q_0(T), q_1(T), \dots, q_{k-1}(T) \in K[T]$  with the required property. By 1.4.3 we have

$$(*_3) \quad \bar{c}(X)_i \in K[X_0, X_1, \dots, X_{k-1}], \quad 0 \leq i < p^k, \quad \text{and} \quad \bar{c}(X)_{p^k} - X_k \in K[X_0, X_1, \dots, X_{k-1}].$$

Write  $N^{p^k} = (c_{ij})$ ,  $1 \leq i, j \leq n$ , and suppose  $\text{ht}(N^{p^k}) = s$ , where  $r < s \leq n - 1$ . Let  $c = c_{i'j'}$  be a *non-zero* coordinate of  $N^{p^k}$  of height  $j' - i' = s$ . Using  $(*_1)$ ,  $(*_2)$ , and  $(*_3)$ , we obtain

$$cX_k - a_{i'j'}(X) = P(X_0, X_1, \dots, X_{k-1}) \in K[X_0, X_1, \dots, X_{k-1}].$$

Now define

$$q_k(T) = c^{-1} (T_{i'j'} + P(q_0(T), q_1(T), \dots, q_{k-1}(T))) \in K[T].$$

Then  $q_k(a) = c^{-1} (a_{i'j'} + P(y_0, y_1, \dots, y_{k-1})) = y_k$ , from which the result follows.  $\square$

We can now prove the main result of this section.

**Theorem 1.6.4** *Let  $K$  be an algebraically closed field of characteristic  $p > 0$ . Suppose  $0 \neq N \in u(n, K)$ ,  $n \geq 2$ , satisfies  $p\text{-nilp}(N) = t \in \mathbb{N}$ . Write  $V = \phi(W_t(K))$ . Then the map*

$$\begin{aligned} \phi : W_t(K) &\rightarrow V \\ y &\mapsto e_p(N, y) \end{aligned}$$

*defined in (29) is an isomorphism of algebraic groups.*

**Proof** That  $\phi$  is a morphism of algebraic groups has already been established (see p.42).

Now suppose  $y = (y_0, y_1, \dots, y_{t-1}) \in W_t(K)$  satisfies

$$(*_1) \quad e_p(N, y) = \sum_{i=0}^{p^t-1} \bar{c}(y)_i N^i = I_n.$$

Let  $1 \leq j \leq t$ . By 1.4.3(i) and (ii), we have  $\bar{c}(X)_0 = 1$ ,  $\bar{c}(X)_1 = X_0$ , and

$$\bar{c}(X)_i = P_i(X_0, X_1, \dots, X_{j-1}) \in K[X_0, X_1, \dots, X_{j-1}]_0, \quad 1 \leq i < p^j.$$

It follows that

$$(*_2) \quad \bar{c}(y)_0 = 1, \quad \bar{c}(y)_1 = y_0, \quad \text{and} \quad \bar{c}(y)_i = P_i(y_0, y_1, \dots, y_{j-1}), \quad 1 \leq i < p^j.$$

Suppose  $e \in \mathbb{N}$  satisfies  $N^e = 0$ , whilst  $N^i \neq 0$ ,  $1 \leq i < e$  (so that  $p^{t-1} < e \leq p^t$ ). Using  $(\ast_1)$  and  $(\ast_2)$ , we obtain

$$(\ast_3) \quad y_0 N + \bar{c}(y)_2 N^2 + \bar{c}(y)_3 N^3 + \cdots + \bar{c}(y)_{e-1} N^{e-1} = 0,$$

where by 1.6.2(i),

$$(\ast_4) \quad 1 \leq \text{ht}(N) < \text{ht}(N^2) < \text{ht}(N^3) < \cdots < \text{ht}(N^e) = n.$$

Write  $N = (a_{ij})$ ,  $1 \leq i, j \leq n$ , and suppose  $\text{ht}(N) = r$ , where  $1 \leq r \leq n-1$ . Let  $a = a_{ij}$  be a *non-zero* coordinate of  $N$  of height  $j-i = r$ . Then by  $(\ast_3)$  and  $(\ast_4)$ , we obtain  $ay_0 = 0$ , and so  $y_0 = 0$ . Now let  $t \geq 2$ ,  $1 \leq k \leq t-1$ , and assume by induction that  $y_0 = y_1 = \cdots = y_{k-1} = 0$ . Putting  $j = k$  into  $(\ast_2)$  gives

$$\bar{c}(y)_i = P_i(y_0, y_1, \dots, y_{k-1}), \quad 1 \leq i < p^k.$$

It follows that  $\bar{c}(y)_i = 0$  for all  $1 \leq i < p^k$ . Now by 1.4.3(iii), we have

$$\bar{c}(X)_{p^k} - X_k = Q_k(X_0, X_1, \dots, X_{k-1}) \in K[X_0, X_1, \dots, X_{k-1}]_0.$$

Therefore  $\bar{c}(y)_{p^k} - y_k = Q_k(y_0, y_1, \dots, y_{k-1})$ . This forces  $\bar{c}(y)_{p^k} = y_k$ , and so  $(\ast_1)$  gives

$$y_k N^{p^k} + \bar{c}(y)_{p^k+1} N^{p^k+1} + \cdots + \bar{c}(y)_{e-1} N^{e-1} = 0.$$

Using  $(\ast_4)$ , and arguing as above, we obtain  $y_k = 0$ . It follows that  $y = 0$ , and  $\phi$  is *injective*.

Therefore  $\phi$  is a bijective morphism of algebraic groups. By 1.6.3, the inverse map

$$\begin{aligned} \phi^{-1} : V &\rightarrow W_t(K) \\ e_p(N, y) &\mapsto y \end{aligned},$$

is a morphism of varieties, and so  $\phi$  is an isomorphism of algebraic groups, as required.  $\square$

We can extend 1.6.4 to an *arbitrary* nilpotent matrix  $0 \neq N' \in M(n, K)$ ,  $n \geq 2$ . Indeed there exists  $P \in GL(n, K)$  such that  $N = PN'P^{-1} \in u(n, K)$ . Suppose  $p\text{-nilp}(N) = p\text{-nilp}(N') = t \in \mathbb{N}$ , and let  $\phi : W_t(K) \rightarrow V$  be the isomorphism  $y \mapsto e_p(N, y)$  above. Since conjugation by  $P^{-1}$  is an isomorphism of  $GL(n, K)$ , restriction to  $V$  yields an isomorphism  $\psi : V \rightarrow W = \psi(V)$ , where  $e_p(N, y) \mapsto e_p(N', y)$ ,  $y \in W_t(K)$ . Thus we have a composition

$$W_t(K) \xrightarrow{\phi} V \xrightarrow{\psi} W,$$

which is an isomorphism of algebraic groups.

## 1.7 Complex Artin-Hasse Exponentials

In this section we introduce an Artin-Hasse-type exponential for nilpotent matrices defined over  $\mathbb{C}$ , and show how to ‘transfer’ this from  $\mathbb{C}$  to  $K$ , a field of characteristic  $p > 0$ . We shall require the following facts: Let  $R, S$  be two commutative rings with identity, and  $\sigma : R \rightarrow S$  a unital ring homomorphism. For  $f(T) = \sum_{i=0}^{\infty} \lambda_i T^i \in R[[T]]$ , define  $f^\sigma(T) = \sum_{i=0}^{\infty} \sigma(\lambda_i) T^i \in S[[T]]$ . Then for  $g(T) \in R[[T]]_0$ , we have

$$(*_1) \quad (f \circ g)^\sigma(T) = (f^\sigma \circ g^\sigma)(T)$$

(compare with (14)). Next let  $0 \neq N \in M(n, R)$ ,  $n \geq 1$ , be nilpotent, with  $N^e = 0$  and  $N^i \neq 0$ ,  $1 \leq i < e$ . As in section 6, define  $f(N) = \sum_{i=0}^{e-1} \lambda_i N^i \in M(n, R)$  (and similarly for  $g(N)$ , etc). Then  $g(N)$  is *nilpotent*, and

$$(*_2) \quad (f \circ g)(N) = f(g(N))$$

(see p.23 and p.40). Finally note that the map  $\sigma$  above induces a ring homomorphism

$$\begin{aligned} \sigma_n : M(n, R) &\rightarrow M(n, S) \\ (a_{ij}) &\mapsto (\sigma(a_{ij})) \end{aligned},$$

satisfying  $\sigma_n(\lambda(a_{ij})) = \sigma(\lambda)\sigma_n(a_{ij})$ ,  $\lambda \in R$ .

Write  $A = \mathbb{Q}[X] = \mathbb{Q}[X_0, X_1, X_2, \dots]$ . For a fixed prime  $p \in \mathbb{N}$ , we have defined (see (23))

$$d(X)_0 = X_0 \text{ and } d(X)_i = \frac{1}{p^i} X_0^{p^i} + \frac{1}{p^{i-1}} X_1^{p^{i-1}} + \dots + \frac{1}{p} X_{i-1}^p + X_i, \quad i \geq 1,$$

and also

$$d(X, T) = \sum_{i=0}^{\infty} d(X)_i T^{p^i} \in A[[T]].$$

Exponentiating this gives

$$\exp(d(X, T)) = \sum_{i=0}^{\infty} c(X)_i T^i,$$

where by 1.4.3(i) and (ii),

$$c(X)_i \in \mathbb{Z}_{(p)}[X_0, X_1, \dots, X_{j-1}], \quad j \geq 1, \quad 0 \leq i < p^j.$$

Let  $0 \neq N \in M(n, \mathbb{Z}_{(p)})$ ,  $n \geq 2$ , be nilpotent, and suppose  $p\text{-nilp}(N) = t \in \mathbb{N}$ . Applying  $(*_2)$ , with  $R = A$ ,  $f(T) = \exp(T)$ , and  $g(T) = d(X, T)$ , gives

$$E(X) = \exp(d(X, N)) = \sum_{i=0}^{p^t-1} c(X)_i N^i \in M(n, \mathbb{Z}_{(p)}[X]),$$

where  $d(X, N) = \sum_{i=0}^{t-1} d(X)_i N^{p^i}$ . We can now introduce an Artin-Hasse-type exponential over  $\mathbb{C}$ . Fix  $x = (x_0, x_1, \dots, x_{t-1}) \in W_t(\mathbb{C})$ , and extend arbitrarily to an element  $\hat{x} = (x_i) \in W(\mathbb{C})$ . Given  $q(X) \in \mathbb{Q}[X]$  we can substitute  $x_i$  for  $X_i$ ,  $i \geq 0$ , to obtain an element  $q(\hat{x}) \in \mathbb{C}$ . Let  $\sigma : \mathbb{Q}[X] \rightarrow \mathbb{C}$  denote the resulting ring homomorphism. Now take  $R = \mathbb{Q}[X]$ ,  $S = \mathbb{C}$ , and  $f(T)$ ,  $g(T)$  as above. Using  $(*)_1$  and  $(*)_2$  we obtain  $f^\sigma(g^\sigma(N)) = (f \circ g)^\sigma(N)$ . Therefore

$$E(x) = \exp(d(x, N)) = \sum_{i=0}^{p^t-1} c(x)_i N^i \in M(n, \mathbb{C}),$$

where  $d(x, N) = \sum_{i=0}^{t-1} d(x)_i N^{p^i}$  (since  $d(\hat{x}, N)$  and  $c(\hat{x})_i$ ,  $0 \leq i \leq p^t - 1$ , only depend on  $x = (x_0, x_1, \dots, x_{t-1})$ , we may write  $d(x, N) = d(\hat{x}, N)$  and  $c(x)_i = c(\hat{x})_i$ ). We have  $E(x) = \sigma_n(E(X))$ .

Next we transfer to  $K$ , a field of characteristic  $p > 0$ . Let  $\psi : \mathbb{Z}_{(p)}[X] \rightarrow K[X]$  denote the natural homomorphism, where  $a/b \mapsto (a \cdot 1)(b \cdot 1)^{-1}$ ,  $a/b \in \mathbb{Z}_{(p)}$ , and  $X_i \mapsto X_i$ ,  $i \geq 0$ . Suppose  $\bar{N} = \psi_n(N) \neq \bar{0}$ , then  $p\text{-nilp}(\bar{N}) = s$ , where  $1 \leq s \leq t$ . Fix  $y = (y_0, y_1, \dots, y_{s-1}) \in W_s(K)$ .

Now

$$\bar{E}(X) = \psi_n(E(X)) = \sum_{i=0}^{p^s-1} \bar{c}(X)_i \bar{N}^i \in M(n, K[X_0, X_1, \dots, X_{s-1}]).$$

Substituting  $y_i$  for  $X_i$ ,  $0 \leq i \leq s-1$ , determines a ring homomorphism, which we denote by  $\bar{\sigma} : K[X_0, X_1, \dots, X_{s-1}] \rightarrow K$ . We have

$$\bar{E}(y) = \bar{\sigma}_n(\bar{E}(X)) = \sum_{i=0}^{p^s-1} \bar{c}(y)_i \bar{N}^i = e_p(\bar{N}, y),$$

the Artin-Hasse exponential of  $\bar{N}$  with respect to  $y$ , as defined in (27).

In the next chapter we apply the results of chapter 1 to the generalized problem, stated on p.3.



## Chapter 2

# Simple Algebraic Groups

In this chapter we apply the techniques developed so far to the generalized problem, stated on p.3. In light of the previous chapter, we can now refine this question, and ask:

**Generalized Problem (GP)** *Let  $G$  be a reductive algebraic group defined over an algebraically closed field  $K$  of characteristic  $p > 0$ . Let  $1 \neq u \in G_u$  be unipotent, with  $\text{o}(u) = p^t$ ,  $t \in \mathbb{N}$ . Under what conditions on  $(u, p)$  does there exist a closed subgroup  $V$  of  $G$ , with  $V \cong W_t(K)$  and  $u \in V$ ?*

Before attacking the GP for an *arbitrary* unipotent element, we first concentrate on the important class of so-called *regular* unipotent elements. These are introduced in 2.1, where their (well-known) characterizations and general properties are discussed. This section also introduces some useful notation, which will be used throughout this chapter. In 2.2 – 2.8 we turn our attention to the various *simple* algebraic groups (the general case is presented in chapter 3).

## 2.1 Regular Unipotent Elements

Assume throughout this section that  $G$  is a (connected) *semisimple* algebraic group defined over an algebraically closed field  $K$  of characteristic  $p \geq 0$ . Choose a maximal torus  $T$  of  $G$ , and let  $B$  be a Borel subgroup of  $G$  containing  $T$ . Then  $U = B_u$  is a closed connected normal subgroup of  $B$ , and we have a semidirect product (of algebraic groups)  $B = U \rtimes T$ . Moreover  $U$  is a maximal connected unipotent subgroup of  $G$ , and all such subgroups are conjugate in  $G$ . Let  $\Phi = \Phi(G, T)$  denote the root system of  $G$  relative to  $T$ , and let  $X_\alpha$  denote the root subgroup of  $G$  corresponding to the root  $\alpha \in \Phi$ . The *positive* root subgroups  $X_\alpha$ ,  $\alpha \in \Phi^+$ , are the non-trivial minimal closed subgroups of  $U$  normalized by  $T$  (the *negative* root subgroups are obtained in the same way from the unique Borel subgroup  $B^-$  opposite to  $B$ ). The root subgroups are 1-dimensional connected unipotent groups, and so for each  $\alpha \in \Phi$ , we have isomorphisms (of algebraic groups)

$$\begin{aligned} x_\alpha : \mathbb{G}_a &\rightarrow X_\alpha \\ \lambda &\mapsto x_\alpha(\lambda) \end{aligned}.$$

These isomorphisms satisfy  $tx_\alpha(\lambda)t^{-1} = x_\alpha(\alpha(t)\lambda)$ ,  $t \in T$ . The product map

$$\phi : \prod_{\alpha \in \Phi^+} X_\alpha \rightarrow U$$

is an isomorphism of varieties, the product of the (positive) root subgroups taken in any (fixed) order. Thus given a fixed ordering of the positive root subgroups, each element  $u \in U$  is expressible *uniquely* as a product

$$u = \prod_{\alpha \in \Phi^+} x_\alpha(\lambda_\alpha), \quad \lambda_\alpha \in K, \quad \alpha \in \Phi^+.$$

Let  $\text{rk}(G)$  denote the dimension of any maximal torus of  $G$ . We now consider the centralizers of elements of  $G$ . Let  $x \in G$ . It is shown in [Sp1] that  $Z_G(x)$  contains a closed abelian subgroup  $A$ , with  $\dim(A) \geq \text{rk}(G)$ . As a consequence we have  $\dim Z_G(x) \geq \text{rk}(G)$  for all  $x \in G$ . An element  $x \in G$  will be called *regular* if  $\dim Z_G(x) = \text{rk}(G)$  (such elements always exist). If  $x \in G$  is regular then  $Z_G(x)^\circ$  is *abelian*. In general we have, for an arbitrary  $x \in G$ ,

$$\dim Z_G(x) = \text{rk}(G) + 2e(x),$$

with  $e(x) = \dim \mathcal{B}_x$ , where  $\mathcal{B}_x$  is the variety of Borel subgroups containing  $x$ . The element  $x$  is called  $e(x)$ -regular. The 0-regular elements are the regular elements; the 1-regular elements are called *subregular*.

We shall be mainly interested in the regular *unipotent* elements of  $G$ . Such elements always exist in  $G$ . Indeed if  $\mathcal{U} = G_u$  denotes the unipotent variety of  $G$ , then the regular unipotent elements of  $G$  form a single conjugacy class  $\mathcal{U}_{reg}$ , which is a (dense) open subset of  $\mathcal{U}$ . The following theorem characterizes the regular unipotent elements of  $G$ . Since every unipotent element of  $G$  is conjugate to an element of  $U$ , it suffices to work entirely inside  $U$ . Let  $\Delta \subseteq \Phi^+$  denote the *simple* roots.

**Theorem 2.1.1** [C2,5.1.3], [H3,4.1;4.6] *Let  $u \in U$  then we have:*

$$u \text{ is regular} \quad \Leftrightarrow \quad u = \prod_{\alpha \in \Phi^+} x_\alpha(\lambda_\alpha) \text{ with } \lambda_\alpha \neq 0 \text{ for all } \alpha \in \Delta .$$

We next consider some useful facts concerning the centralizers of regular unipotent elements of  $G$ . Let  $u \in U$  be regular. Write  $Z = Z(G)$  and  $r = \text{rk}(G)$ . It can be shown that

$$Z_G(u) = Z_U(u)Z \quad \text{and} \quad Z_G(u)^\circ = Z_U(u)^\circ$$

(see [Sp2,4.3]). In particular, it follows that  $Z_G(u)^\circ$  is an  $r$ -dimensional closed connected abelian unipotent subgroup of  $G$ . Now suppose there exists a closed connected abelian subgroup  $V$  of  $G$ , with  $u \in V$ . Then  $V \subseteq Z_U(u)^\circ$ , and so  $V$  is unipotent, with  $\dim(V) \leq r$ . We also obtain  $u \in Z_U(u)^\circ$ . In this direction we have the following result. Refer to p.2 for the definitions of good and bad primes.

**Theorem 2.1.2** [Sp2,4.11;4.12] *Let  $u \in U$  be regular. Then the following hold:*

- (i) *Let  $p = 0$  or a good prime for  $G$ . Then  $Z_U(u)$  is connected.*
- (ii) *If  $p$  is a bad prime for  $G$ , then  $u \notin Z_U(u)^\circ$ . Moreover  $Z_U(u) = \langle u, Z_U(u)^\circ \rangle$ .*

As an immediate consequence of this result, and the above remarks, we have

**Corollary 2.1.3** *Let  $u \in \mathcal{U} = G_u$  be regular, and assume that  $p$  is a bad prime for  $G$ . Then  $u$  does not lie in any closed connected abelian subgroup of  $G$ .*

Therefore the GP *fails* for pairs  $(u, p)$ , where  $u \in \mathcal{U}$  is regular, and  $p$  is a bad prime for  $G$ . From now on, we shall only consider the GP under the assumption that  $p$  is a *good* prime for  $G$  (this of course leaves undecided the cases  $(u, p)$ , where  $u$  is not regular and  $p$  is bad). Note that 2.1.3 holds when  $G$  is reductive, since  $G'$  is semisimple (see p.123 to follow).

Before commencing our study of regular unipotent elements in *simple* algebraic groups, we first need to introduce some standard notation. The simple algebraic groups considered shall be viewed as Chevalley groups, each corresponding to one of the various simple Lie algebras. For the theory of such groups, consult [St] and [Cu]. Let  $L$  be such a Lie algebra, and let  $\Phi$  denote the set of roots of  $L$ , with  $\Phi^+$  and  $\Phi^-$  denoting, respectively, the positive and negative roots relative to some base. Following [R] and [C1,11.3], a particularly nice  $(n \times n)$  matrix representation of  $L$  is chosen, in which the root vectors  $e_\alpha$ ,  $\alpha \in \Phi$ , of a Chevalley basis satisfy the following condition: Let  $X$  be an indeterminate, then  $\exp(Xe_\alpha) \in M(n, \mathbb{Z}[X])$ . Now let  $K$  be an algebraically closed field of characteristic  $p > 0$ . For  $\mu \in K$ , let  $x_\alpha(\mu)$  denote the matrix in  $M(n, K)$  obtained from  $\exp(Xe_\alpha)$  by replacing each ‘coordinate’  $f(X) \in \mathbb{Z}[X]$  by  $\bar{f}(\mu) \in K$ , where  $\bar{f}(X)$  is the image of  $f(X)$  under the natural homomorphism  $\mathbb{Z}[X] \rightarrow K[X]$ . Define  $X_\alpha = \{x_\alpha(\mu) : \mu \in K\}$ , a subgroup of  $SL(n, K)$ . Then the corresponding Chevalley group is the subgroup  $G(K)$  of  $SL(n, K)$  generated by all  $X_\alpha$ ,  $\alpha \in \Phi$ . Write  $G = G(K)$  for brevity. Associated with  $G$  are the following important subgroups:

$$(CG1) \quad U = \langle X_\alpha : \alpha \in \Phi^+ \rangle, \quad T = \langle h_\alpha(t) : \alpha \in \Phi, t \in \mathbb{G}_m \rangle, \quad \text{and} \quad B = \langle U, T \rangle$$

(for the definition of  $h_\alpha(t)$ , consult [St,p.27]). It can be shown that  $B = U \rtimes T$  is a Borel subgroup of  $G$ ,  $U = B_u$  is a maximal connected unipotent subgroup of  $G$ , and  $T$  is a maximal torus of  $G$ . The  $X_\alpha$ ,  $\alpha \in \Phi^+$ , are the non-trivial minimal subgroups of  $U$  normalized by  $T$ , and so are the positive root subgroups. The negative root subgroups are obtained from the subgroup  $U^-$  of  $G$  generated by all  $X_\alpha$ ,  $\alpha \in \Phi^-$ . For each  $\alpha \in \Phi$ , the map

$$(CG2) \quad \begin{array}{ccc} x_\alpha : \mathbb{G}_a & \rightarrow & X_\alpha \\ \mu & \mapsto & x_\alpha(\mu) \end{array}$$

is an isomorphism of algebraic groups.

## 2.2 Type $A_l$

Let  $L = sl(l+1, \mathbb{C})$ ,  $l \geq 1$ , be the set of all  $(l+1) \times (l+1)$  matrices of trace 0 over  $\mathbb{C}$ . Then (under commutation)  $L$  is the complex simple Lie algebra of type  $A_l$ . We now give a brief description of  $L$ , following [B2,VIII,13], [C1,11.2], and [J1,IV,6], which should also be consulted for the other types. Also consult p.vi for the various Dynkin diagrams. Let  $H$  be the set of all  $(l+1) \times (l+1)$  diagonal matrices in  $L$ . Then  $H$  is a Cartan subalgebra of  $L$  (of  $l$  dimensions). The elements of  $H$  have the form

$$h = \begin{pmatrix} \lambda_1 & & & \\ & \ddots & & \\ & & \lambda_l & \\ & & & \lambda_{l+1} \end{pmatrix}, \quad -\lambda_{l+1} = \sum_{i=1}^l \lambda_i.$$

A basis for  $L$  is

$$\begin{aligned} h_i &= e_{ii} - e_{l+1,l+1}, & 1 \leq i \leq l. \\ e_{ij}, & & i \neq j = 1, 2, \dots, l+1. \end{aligned}$$

For  $h = \sum_{i=1}^l \lambda_i h_i \in H$  we have

$$[h, e_{ij}] = (\lambda_i - \lambda_j) e_{ij}, \quad i \neq j = 1, 2, \dots, l+1.$$

Let  $i \neq j = 1, 2, \dots, l+1$ . Then the  $l^2 + l$  linear transformations  $\alpha_{ij} : H \rightarrow \mathbb{C}$  arising above, where  $h \xrightarrow{\alpha_{ij}} \lambda_i - \lambda_j$ , are the roots of  $L$  (relative to  $H$ ). The set of roots will be denoted by  $\Phi = \Phi(L, H)$ . Each root  $\alpha_{ij}$  will be identified with its corresponding element  $\lambda_i - \lambda_j \in \mathbb{C}$ . The elements

$$\alpha_1 = \lambda_1 - \lambda_2, \quad \alpha_2 = \lambda_2 - \lambda_3, \quad \dots, \quad \alpha_{l-1} = \lambda_{l-1} - \lambda_l, \quad \alpha_l = \lambda_l - \lambda_{l+1},$$

(where  $\alpha_i = \alpha_{i,i+1}$ ,  $1 \leq i \leq l$ ) then form a set  $\Delta$  of *simple* roots of  $L$  (relative to  $H$ ). The set  $\Phi^+$  of *positive* roots consists of all roots of the form

$$\alpha_{ij} = \lambda_i - \lambda_j = \alpha_i + \dots + \alpha_{j-1}, \quad 1 \leq i < j \leq l+1.$$

We have  $1 \leq \text{ht}(\alpha_{ij}) = j - i \leq l$ . There are  $l+1-i$  roots of height  $i$ ,  $1 \leq i \leq l$ , the *highest* root being

$$r_0 = \alpha_{1,l+1} = \alpha_1 + \alpha_2 + \dots + \alpha_l,$$

of height  $\text{ht}(r_0) = l$ . Moreover  $|\Phi^+| = l(l+1)/2$ .

Next we introduce some useful notation, which is a modification of that used in 1.6. Let  $R$  be a commutative ring with identity. Define  $u(n, R) = \{(a_{ij}) \in M(n, R) : a_{ij} = 0, i \geq j\}$ ,  $n \geq 1$ , the set of all strictly upper triangular matrices over  $R$  (compare with 1.6). Let  $0 \neq A \in u(n, R)$ ,  $n \geq 2$ . We will write  $\text{ht}(A) = r$ ,  $1 \leq r \leq n-1$ , if  $A$  is of the form

$$A = \sum_{i=1}^{n-r} \lambda_i e_{i, i+r}, \quad \lambda_i \in R, \quad 1 \leq i \leq n-r, \quad \text{not all zero.}$$

Now let  $\alpha = \alpha_{ij} \in \Phi^+$ ,  $1 \leq i < j \leq l+1$ , and write  $e_\alpha = e_{ij}$  for ‘the’ root vector corresponding to  $\alpha$ . Then

$$\text{ht}(e_\alpha) = j - i = \text{ht}(\alpha).$$

This reflects the fact that the root vectors corresponding to the simple roots are of height 1. For convenience we list below the *positive* root vectors in order of increasing height:

<u>Height</u>	<u>Corresponding Root Vectors</u>	<u>Number</u>
1	$e_{i, i+1}, \quad 1 \leq i \leq l$	$l$
2	$e_{i, i+2}, \quad 1 \leq i \leq l-1$	$l-1$
3	$e_{i, i+3}, \quad 1 \leq i \leq l-2$	$l-2$
$\vdots$	$\vdots$	$\vdots$
$l$	$e_{1, l+1}$	$1$

(†) *We now fix the following notation to be used throughout this chapter:* Let  $K$  be a field of characteristic  $p > 0$ , and  $K[X] = K[X_0, X_1, \dots, X_{t-1}]$ ,  $t \in \mathbb{N}$ . Write  $\psi : \mathbb{Z}_{(p)}[X] \rightarrow K[X]$  for the natural homomorphism, and for  $n \geq 1$ , let  $\psi_n : M(n, \mathbb{Z}_{(p)}[X]) \rightarrow M(n, K[X])$  denote the induced matrix homomorphism (also see 1.7). Given  $A \in M(n, \mathbb{Z}_{(p)}[X])$ , we shall write  $\overline{A} = \psi_n(A)$ .

In the following elementary result, we consider *powers* of matrices (as opposed to commutators):

**Lemma 2.2.1** *Let  $n \geq 2$  and suppose*

$$N = \sum_{i=1}^{n-1} \lambda_i e_{i, i+1} \in M(n, \mathbb{Z}), \quad \text{with } \lambda_i \in \mathbb{Z} - p\mathbb{Z}, \quad 1 \leq i \leq n-1$$

(so that  $\text{ht}(N) = 1$ ). Then the following hold:

(a)

$$N^r = \sum_{i=1}^{n-r} \left( \prod_{j=0}^{r-1} \lambda_{i+j} \right) e_{i,i+r} \in M(n, \mathbb{Z}), \quad 1 \leq r \leq n-1,$$

(so  $\text{ht}(N^r) = r$ ), with  $\prod_{j=0}^{r-1} \lambda_{i+j} \in \mathbb{Z} - p\mathbb{Z}$ ,  $1 \leq i \leq n-r$ . Moreover  $N^r = 0$ ,  $r \geq n$ .

(b) Write  $\bar{N} = \psi_n(N)$ . Then  $p\text{-nilp}(\bar{N}) = p\text{-nilp}(N) = t$ , where  $p^{t-1} < n$  and  $p^t \geq n$ .

**Proof** (a) The result is clearly true for  $r = 1$ . Let  $r \geq 2$  and assume

$$N^{r-1} = \sum_{i=1}^{n-(r-1)} \left( \prod_{j=0}^{(r-1)-1} \lambda_{i+j} \right) e_{i,i+(r-1)} \quad \text{if } 2 \leq r \leq n,$$

and  $N^{r-1} = 0$  if  $r > n$ . Recall

$$(*) \quad e_{ij}e_{kl} = \delta_{jk}e_{il}, \quad 1 \leq i, j, k, l \leq n.$$

If  $r > n$  then  $N^r = 0$ , so assume  $2 \leq r \leq n$ . We have

$$N^r = N N^{r-1} = \left( \sum_{i=1}^{n-1} \lambda_i e_{i,i+1} \right) \left( \sum_{i=1}^{n-r+1} \left( \prod_{j=0}^{r-2} \lambda_{i+j} \right) e_{i,i+r-1} \right).$$

If  $r = n$  then  $(*)$  gives  $N^r = 0$ . Now suppose  $n \geq 3$  and  $2 \leq r \leq n-1$ . Then  $(*)$  gives

$$N^r = \sum_{i=1}^{n-r} \lambda_i \left( \prod_{j=0}^{r-2} \lambda_{i+1+j} \right) e_{i,i+r} = \sum_{i=1}^{n-r} \left( \prod_{j=0}^{r-1} \lambda_{i+j} \right) e_{i,i+r},$$

as required.

(b) Apply the map  $\psi_n$ , to obtain  $N^r = 0$  if and only if  $\bar{N}^r = \bar{0}$ ,  $r \in \mathbb{N}$ . □

The following result is then clear, and is to be expected in light of the above remarks:

**Corollary 2.2.2** *Let*

$$N = \sum_{\text{ht}(\alpha)=1} e_\alpha = e_{\alpha_1} + e_{\alpha_2} + \cdots + e_{\alpha_l} \in L = \mathfrak{sl}(l+1, \mathbb{C}), \quad l \geq 1.$$

*Then we have*

$$N^r = \sum_{\text{ht}(\alpha)=r} e_\alpha, \quad 1 \leq r \leq l,$$

*and*  $N^r = 0$ ,  $r > l$ . *In particular,*  $N^{\text{ht}(r_0)} = e_{r_0}$ .

**Proof** Let  $n = l + 1$  in 2.2.1, and use the table of positive root vectors given above.  $\square$

Let  $K$  be an algebraically closed field of characteristic  $p > 0$ . We now introduce the Chevalley group  $G(K)$  corresponding to  $L$ . For  $\alpha \in \Phi$  let  $h_\alpha$  denote the *coroot* corresponding to  $\alpha$ . Then the set  $\{h_{\alpha_i}, e_\alpha : \alpha_i \in \Delta, \alpha \in \Phi\}$  is a *Chevalley basis* of  $L$  (see [H1, VII] for the definitions). In the notation of 2.1 (see p.52), we have for  $t_i, t_\alpha \in K$ ,

$$(**) \quad \begin{aligned} x_{\alpha_i}(t_i) &= \bar{I} + t_i \bar{e}_{i, i+1}, & \alpha_i \in \Delta, \quad 1 \leq i \leq l, \\ x_\alpha(t_\alpha) &= \bar{I} + t_\alpha \bar{e}_{ij}, & \alpha = \alpha_{ij} \in \Phi^+ - \Delta, \quad 1 \leq i < j - 1 \leq l \end{aligned}$$

(see (†) for the bar notation). Recall  $X_\alpha = \{x_\alpha(t) : t \in K\}$  and  $G(K) = \langle X_\alpha : \alpha \in \Phi \rangle$ . It is shown in [R] that  $G(K) = SL(l + 1, K)$ ; it is the *simply-connected* simple algebraic group of type  $A_l$  defined over  $K$ . Write  $G = G(K)$  for brevity. In this case, the subgroups of  $G$  as defined in (CG1) of 2.1 are:

$$U = U(l + 1, K), \quad T = SL(l + 1, K) \cap D(l + 1, K), \quad \text{and} \quad B = SL(l + 1, K) \cap B(l + 1, K).$$

Here  $D(l + 1, K)$  and  $B(l + 1, K)$  are, respectively, the sets of diagonal and upper triangular matrices in  $GL(l + 1, K)$ . For a more direct account of the group  $SL(l + 1, K)$ , including the (global) roots of  $G$  relative to  $T$ , consult [DM, 15.1].

We now concentrate on the unipotent elements of  $G = SL(l + 1, K)$ . Since the maximal connected unipotent subgroups of  $G$  are all conjugate, we can restrict our attention to the subgroup  $U = U(l + 1, K)$ . Each element  $u \in U$  is of the form

$$u = \begin{pmatrix} 1 & \mu_1 & * & & \cdots & * \\ & 1 & \mu_2 & * & & \vdots \\ & & \ddots & \ddots & \ddots & \\ & & & & & * \\ & & & & & \mu_l \\ & & & & & 1 \end{pmatrix}.$$

We shall write  $u(1) = (\mu_1, \mu_2, \dots, \mu_l)$ , and call this the *superdiagonal* of  $u$  (we can think of  $u(1)$  as the ‘vector’ of height 1 elements of  $u$ ). The following result is well-known:

**Lemma 2.2.3** *Let  $u \in U = U(l + 1, K)$ , and suppose  $u(1) = (\mu_1, \mu_2, \dots, \mu_l)$ , for some  $\mu_i \in K$ ,  $1 \leq i \leq l$ . Then*

$$u \text{ is regular} \quad \Leftrightarrow \quad \mu_i \neq 0 \quad \text{for all } i = 1, 2, \dots, l.$$



**Proof** We can see this (indirectly) as follows: From 2.1 we know that  $u$  can be written (uniquely) as a product

$$u = x_{\alpha_1}(t_1)x_{\alpha_2}(t_2)\cdots x_{\alpha_l}(t_l) \prod_{\alpha \in \Phi^+ - \Delta} x_{\alpha}(t_{\alpha}) ,$$

for some  $t_i, t_{\alpha} \in K$  (the product has been taken in this order for convenience only; indeed the coefficients  $t_i$ ,  $1 \leq i \leq l$ , do not depend on the order). Using (\*\*) above, it is then clear that  $u(1) = (t_1, t_2, \dots, t_l)$ , and so  $t_i = \mu_i$ ,  $1 \leq i \leq l$ . The result now follows from 2.1.1.  $\square$

We now come to the main result of this section. A complete proof is given as it acts as a model for the subsequent cases. The proof uses notation from 1.7, which should be consulted for more details. Note that the choice of  $N$  below is motivated by 2.2.3. Further motivation is provided by the Campbell-Hausdorff formula, as described in [B3,II,6] and [J1,V,5], but we do not pursue this here.

**Theorem 2.2.4** *Let  $G = SL(l+1, K)$ ,  $l \geq 1$ , where  $K$  is an algebraically closed field of characteristic  $p > 0$ . Suppose  $u \in G_u$  is a regular unipotent element. Then the following hold:*

(i)  $o(u) = p^t = \min \{p^s : s \in \mathbb{N} \text{ and } p^s > \text{ht}(r_0)\}$ .

(ii) *There exists a closed subgroup  $V$  of  $G$ , with  $V \cong W_t(K)$  and  $u \in V$ .*

**Proof** Let  $N = \sum_{\text{ht}(\alpha)=1} e_{\alpha} \in L = \mathfrak{sl}(l+1, \mathbb{C})$ . Then  $0 \neq N$  is nilpotent, with  $p\text{-nilp}(N) = t \in \mathbb{N}$ , where by 2.2.1,

$$p^{t-1} \leq l = \text{ht}(r_0) \text{ and } p^t > l.$$

In the notation of 1.7, we have (for  $X = (X_0, X_1, \dots, X_{t-1})$ )

$$E(X) = \exp(d(X, N)) = \sum_{i=0}^{p^t-1} c(X)_i N^i \in M(l+1, \mathbb{Z}_{(p)}[X]),$$

where  $c(X)_0 = 1$  and  $c(X)_1 = X_0$  (see 1.4.3(i)). We now transfer to  $K$  (see (†) above). By 2.2.1(b), we have  $p\text{-nilp}(\bar{N}) = p\text{-nilp}(N) = t$  (where  $\bar{N} = \psi_{l+1}(N)$ ). Now

$$\bar{E}(X) = \psi_{l+1}(E(X)) = \sum_{i=0}^{p^t-1} \bar{c}(X)_i \bar{N}^i \in M(l+1, K[X]).$$

Fix  $y = (y_0, y_1, \dots, y_{t-1}) \in W_t(K)$ , so that  $\bar{c}(y)_0 = 1$  and  $\bar{c}(y)_1 = y_0$ . Substituting  $y_i$  for  $X_i$ ,  $0 \leq i \leq t-1$ , in  $\bar{E}(X)$  gives

$$\bar{E}(y) = e_p(\bar{N}, y) = \bar{I} + y_0 \bar{N} + \sum_{i=2}^{p^t-1} \bar{c}(y)_i \bar{N}^i \in U = U(l+1, K) \subseteq G = SL(l+1, K).$$

Since  $1 = \text{ht}(\bar{N}) < \text{ht}(\bar{N}^i)$ ,  $2 \leq i \leq p^t - 1$ , the description of  $N$  makes it clear that the superdiagonal  $e_p(\bar{N}, y)(1) = (y_0, y_0, \dots, y_0)$ . Therefore by 2.2.3, we have

$$\begin{aligned} (***) \quad e_p(\bar{N}, y) \text{ is regular} &\Leftrightarrow y_0 \neq 0 \\ &\Leftrightarrow o(y) = p^t \quad (\text{by 1.2.3(c)}) \end{aligned}$$

Now define

$$\begin{aligned} \phi : W_t(K) &\rightarrow SL(l+1, K) \\ y &\mapsto e_p(\bar{N}, y) \end{aligned},$$

and write  $V = \phi(W_t(K))$ . Then by 1.6.4,  $\phi : W_t(K) \rightarrow V$  is an isomorphism of algebraic groups (in particular,  $V$  is a closed subgroup of  $G$  of the required type). Moreover by  $(***)$ ,  $V$  contains a regular unipotent element of  $G$  (many in fact), and since all such elements are conjugate in  $G$  (see 2.1), we obtain:

$$u \in G \text{ regular unipotent} \Rightarrow o(u) = p^t.$$

The result follows since conjugation in  $G$  is an isomorphism of algebraic groups. □

Part (i) of 2.2.4 is well-known. Indeed an ‘order formula’ is known for *every* unipotent element in *every* simple algebraic group. See [T2] and [La] for more details.

## 2.3 Type $C_l$

Let  $L = sp(2l, \mathbb{C})$ ,  $l \geq 3$ , be the set of all  $(2l) \times (2l)$  matrices  $x$  over  $\mathbb{C}$  satisfying

$$x^t A = -Ax,$$

where

$$A = \left( \begin{array}{c|c} 0 & J_l \\ \hline -J_l & 0 \end{array} \right), \quad J_l = \begin{pmatrix} 0 & & 1 \\ & \ddots & \\ 1 & & 0 \end{pmatrix}$$

(we call  $x$  *skew* relative to  $A$ ). Then  $L$  is the complex simple Lie algebra of type  $C_l$ . As in type  $A_l$ , we give below a brief description of  $L$ . Consult 2.2 for the relevant references. Let  $H$  be the set of all  $(2l) \times (2l)$  diagonal matrices in  $L$ . Then  $H$  is a Cartan subalgebra of  $L$  (of  $l$  dimensions). The elements of  $H$  have the form

$$h = \begin{pmatrix} \lambda_1 & & & & & \\ & \ddots & & & & \\ & & \lambda_l & & & \\ & & & -\lambda_l & & \\ & & & & \ddots & \\ & & & & & -\lambda_1 \end{pmatrix}.$$

We will number the rows and columns of the matrices as follows:

$$1, \ 2, \ \dots, \ l-1, \ l, \ l', \ (l-1)', \ \dots, \ 2', \ 1'.$$

The following conversion is clear: Let  $1 \leq i \leq l$  and consider the label  $i'$ . Then  $i'$  represents the  $(2l+1-i)$ -th row or column of a given matrix. Conversely the  $i$ -th row or column, where  $l+1 \leq i \leq 2l$ , is labelled by  $(2l+1-i)'$  in the new notation. A basis for  $L$  is then

$$\begin{aligned} h_i &= e_{ii} - e_{i'i'}, \quad 1 \leq i \leq l. \\ e_{\lambda_i - \lambda_j} &= e_{ij} - e_{j'i'}, \quad 1 \leq i < j \leq l. \\ e_{\lambda_j - \lambda_i} &= e_{ji} - e_{i'j'}, \quad 1 \leq i < j \leq l. \\ e_{\lambda_i + \lambda_j} &= e_{ij'} + e_{ji'}, \quad 1 \leq i < j \leq l. \\ e_{-\lambda_i - \lambda_j} &= e_{j'i} + e_{i'j}, \quad 1 \leq i < j \leq l. \\ e_{2\lambda_i} &= e_{ii'}, \quad 1 \leq i \leq l. \\ e_{-2\lambda_i} &= e_{i'i}, \quad 1 \leq i \leq l. \end{aligned}$$

For  $h = \sum_{i=1}^l \lambda_i h_i \in H$  we have

$$\begin{aligned}
[h, e_{\lambda_i - \lambda_j}] &= (\lambda_i - \lambda_j) e_{\lambda_i - \lambda_j}, \quad 1 \leq i < j \leq l. \\
[h, e_{\lambda_j - \lambda_i}] &= (\lambda_j - \lambda_i) e_{\lambda_j - \lambda_i}, \quad 1 \leq i < j \leq l. \\
[h, e_{\lambda_i + \lambda_j}] &= (\lambda_i + \lambda_j) e_{\lambda_i + \lambda_j}, \quad 1 \leq i < j \leq l. \\
[h, e_{-\lambda_i - \lambda_j}] &= (-\lambda_i - \lambda_j) e_{-\lambda_i - \lambda_j}, \quad 1 \leq i < j \leq l. \\
[h, e_{2\lambda_i}] &= (2\lambda_i) e_{2\lambda_i}, \quad 1 \leq i \leq l. \\
[h, e_{-2\lambda_i}] &= (-2\lambda_i) e_{-2\lambda_i}, \quad 1 \leq i \leq l.
\end{aligned}$$

The  $2l^2$  linear transformations  $H \rightarrow \mathbb{C}$  arising above, where  $h \mapsto \lambda_i - \lambda_j$ ,  $h \mapsto \lambda_j - \lambda_i$ ,  $h \mapsto \lambda_i + \lambda_j$ , etc, are the roots  $\Phi$  of  $L$  (relative to  $H$ ). Each root will be identified with its corresponding subscript in  $\mathbb{C}$ . The elements

$$\alpha_1 = \lambda_1 - \lambda_2, \quad \alpha_2 = \lambda_2 - \lambda_3, \quad \dots, \quad \alpha_{l-1} = \lambda_{l-1} - \lambda_l, \quad \alpha_l = 2\lambda_l,$$

then form a set  $\Delta$  of simple roots of  $L$  (relative to  $H$ ). It is convenient to partition the set  $\Phi^+$  of positive roots into the following three subsets:

$$\begin{aligned}
(1) \quad \Phi_{ij} &= \{\alpha_{ij} = \lambda_i - \lambda_j : 1 \leq i < j \leq l\} \\
(2) \quad \Phi_{ij'} &= \{\alpha_{ij'} = \lambda_i + \lambda_j : 1 \leq i < j \leq l\} \\
(3) \quad \Phi_{ii'} &= \{\alpha_{ii'} = 2\lambda_i : 1 \leq i \leq l\}
\end{aligned}$$

We have

$$\begin{aligned}
(1) \quad \text{ht}(\alpha_{ij}) &= j - i & ; \quad |\Phi_{ij}| &= l(l-1)/2 \\
(2) \quad \text{ht}(\alpha_{ij'}) &= 2l + 1 - j - i & ; \quad |\Phi_{ij'}| &= l(l-1)/2 \\
(3) \quad \text{ht}(\alpha_{ii'}) &= 2l + 1 - 2i & ; \quad |\Phi_{ii'}| &= l
\end{aligned}$$

For each  $\alpha \in \Phi^+$ , we have  $\text{ht}(e_\alpha) = \text{ht}(\alpha)$ , the root vectors corresponding to the simple roots being of height 1, as in type  $A_l$  (see 2.2, p.54, for notation). The total number of positive roots is  $l^2$ . The highest root is

$$\tau_0 = \alpha_{11'} = 2\alpha_1 + \dots + 2\alpha_{l-1} + \alpha_l,$$

of height  $\text{ht}(\tau_0) = 2l - 1$ .

We now concentrate on powers of matrices. The following useful result is well-known:

**Lemma 2.3.1** [C1,11.2.2] *Let  $A, N \in M(n, \mathbb{C})$ ,  $n \geq 1$ , and suppose  $N^t A = -AN$ . Then the following hold:*

(i)  $(N^i)^t A = (-1)^i AN^i$  for all  $i \geq 1$ .

(ii) Suppose  $N$  is nilpotent, then  $(\exp N)^t A (\exp N) = A$ .

Let  $N = \sum_{i=1}^l e_{\alpha_i} \in L = \mathfrak{sp}(2l, \mathbb{C})$ ,  $l \geq 3$ , and suppose  $1 \leq r \leq 2l - 1$ . Then  $N^r \neq 0$  by 2.2.1(a). If  $r$  is even then 2.3.1(i) implies that  $N^r \notin L$ . Indeed if  $N^r \in L$  then  $(N^r)^t A = AN^r = -AN^r$ , and so  $AN^r = 0$ . But  $\det(A) = 1 \neq 0$ , which gives  $N^r = 0$ , a contradiction. For this reason we restrict our attention to the case where  $r$  is odd. This amounts to excluding the bad prime 2 from the main result (2.3.5) of this section. For convenience we list below the positive root vectors of odd height: Let  $r = 2s + 1$  where  $0 \leq s \leq l - 1$  (so that  $1 \leq r \leq 2l - 1$ ). The root vectors will be partitioned into the three subsets defined above.

Case (i)

$$\text{Suppose } 1 \leq r \leq \begin{cases} l - 2 & : l \text{ odd} \\ l - 1 & : l \text{ even} \end{cases}.$$

(1)  $e_{\alpha_{ij}} = e_{ij} - e_{j'i'}, \quad j = i + r,$

where  $1 \leq i \leq l - r$ . There are  $l - r = l - 2s - 1$  root vectors of this form.

(2)  $e_{\alpha_{ij'}} = e_{ij'} + e_{ji'}, \quad j = 2l + 1 - (i + r),$

where  $l - 2s \leq i \leq l - s - 1$ , and  $s \neq 0$ . There are  $s$  root vectors of this form.

(3)  $e_{\alpha_{ii'}} = e_{ii'},$

where  $i = l - s$ . There is 1 root vector of this form.

Case (ii)

$$\text{Suppose } \begin{cases} l \leq r \leq 2l - 1 & : l \text{ odd} \\ l + 1 \leq r \leq 2l - 1 & : l \text{ even} \end{cases}.$$

(1) There is no contribution from this subset.

(2)  $e_{\alpha_{ij'}} = e_{ij'} + e_{ji'}, \quad j = 2l + 1 - (i + r),$

where  $1 \leq i \leq l - s - 1$ , and  $s \neq l - 1$ . There are  $l - s - 1$  root vectors of this form.

$$(3) \quad e_{\alpha_{ii'}} = e_{ii'} ,$$

where  $i = l - s$ . There is 1 root vector of this form.

Note that, in both cases, there are  $l - s$  root vectors (and roots) of height  $2s + 1$ ,  $0 \leq s \leq l - 1$  (also compare with [Sp2]).

For completeness, we now include the analogue of 2.2.2 for the case  $C_l$ :

**Lemma 2.3.2** *Let*

$$N = \sum_{\text{ht}(\alpha)=1} e_{\alpha} = e_{\alpha_1} + \cdots + e_{\alpha_{l-1}} + e_{\alpha_l} \in L = sp(2l, \mathbb{C}), \quad l \geq 3.$$

*Then the following hold:*

(a) *Let  $r = 2s + 1$ , where  $0 \leq s \leq l - 1$ .*

$$\text{Case (i)} \quad \text{Suppose } 1 \leq r \leq \begin{cases} l - 2 & : l \text{ odd} \\ l - 1 & : l \text{ even} \end{cases}, \text{ then}$$

$$N = \sum_{i=1}^{l-1} e_{\alpha_{i,i+1}} + e_{\alpha_{l,l'}} ,$$

$$N^r = \sum_{i=1}^{l-r} e_{\alpha_{i,i+r}} + (-1)^l \sum_{i=l-2s}^{l-s-1} (-1)^i e_{\alpha_{i,(2l+1-i-r)'}} + (-1)^s e_{\alpha_{l-s,(l-s)'}} , \quad s \neq 0.$$

$$\text{Case (ii)} \quad \text{Suppose } \begin{cases} l \leq r \leq 2l - 1 & : l \text{ odd} \\ l + 1 \leq r \leq 2l - 1 & : l \text{ even} \end{cases}, \text{ then}$$

$$N^r = (-1)^l \sum_{i=1}^{l-s-1} (-1)^i e_{\alpha_{i,(2l+1-i-r)'}} + (-1)^s e_{\alpha_{l-s,(l-s)'}} , \quad s \neq l - 1,$$

$$N^{2l-1} = (-1)^{l-1} e_{\alpha_{1,1'}} .$$

*In particular, in both cases, we have  $N^r = \sum_{\text{ht}(\alpha)=r} \lambda_{\alpha} e_{\alpha}$ , where each  $\lambda_{\alpha} \in \{-1, 1\}$  depends on  $l, s$ , and  $\alpha$ , and  $N^{\text{ht}(r_0)} = (-1)^{l-1} e_{r_0}$ .*

(b)  $N^i = 0$  for  $i \geq 2l$ .

**Proof** For convenience, we revert to the (old) notation of numbering rows and columns by  $1, 2, \dots, l, l+1, \dots, 2l-1, 2l$ . Then

$$N = \sum_{i=1}^{2l-1} \lambda_i e_{i,i+1}, \quad \text{where} \quad \lambda_i = \begin{cases} 1 & : 1 \leq i \leq l \\ -1 & : l+1 \leq i \leq 2l-1 \end{cases}.$$

Let  $r = 2s + 1$  where  $0 \leq s \leq l-1$ . Applying 2.2.1(a) (with  $n = 2l$ ) gives

$$N^r = \sum_{i=1}^{2l-r} \left( \prod_{j=0}^{r-1} \lambda_{i+j} \right) e_{i,i+r} \in L,$$

by 2.3.1(i). Moreover  $\text{ht}(N^r) = r$ . Cases (i) and (ii) of part (a) now follow from the description of the height  $r$  root vectors given above. In particular, for  $r = \text{ht}(r_0) = 2l-1$ , we have

$$\begin{aligned} N^{\text{ht}(r_0)} &= \left( \prod_{j=0}^{2l-2} \lambda_{1+j} \right) e_{1,2l} \\ &= (\lambda_1 \dots \lambda_l)(\lambda_{l+1} \dots \lambda_{2l-1}) e_{1,2l} \\ &= (-1)^{l-1} e_{r_0}. \end{aligned}$$

Part (b) is clear. □

We now prove a technical lemma which will be needed for the main result (2.3.5) of this section (and also in the following two sections). Let  $K$  be a field of characteristic  $p > 0$ ,  $n \geq 1$ , and  $X = (X_0, X_1, \dots, X_{t-1})$  for some  $t \in \mathbb{N}$ . Define  $\psi_n : M(n, \mathbb{Z}_{(p)}[X]) \rightarrow M(n, K[X])$  as in (†) of 2.2. Given  $A(X) \in M(n, \mathbb{Z}_{(p)}[X])$  and  $x \in W_t(\mathbb{C})$ , we can substitute  $x$  for  $X$  in  $A(X)$  to obtain a matrix  $A(x) \in M(n, \mathbb{C})$  (and similarly for  $M(n, K[X])$ ).

**Lemma 2.3.3** *Let  $E(X) \in M(n, \mathbb{Z}_{(p)}[X])$  and  $A \in M(n, \mathbb{Z}_{(p)})$ . Write  $\overline{E}(X) = \psi_n(E(X))$  and  $\overline{A} = \psi_n(A)$ . Suppose*

$$E(x)^t A E(x) = A, \quad \text{for all } x \in W_t(\mathbb{C}).$$

*Then*

$$\overline{E}(y)^t \overline{A} \overline{E}(y) = \overline{A}, \quad \text{for all } y \in W_t(K).$$

**Proof** Let  $1 \leq i, j \leq n$  and write  $A = (a_{ij})$ . The  $(i, j)$ -th coefficient of  $E(X)^t A E(X)$  is of the form  $P_{ij}(X) \in \mathbb{Z}_{(p)}[X]$ . By assumption, the polynomial  $P_{ij}(X) - a_{ij}$  vanishes for

all  $x \in W_t(\mathbb{C})$ . This forces  $P_{ij}(X) = a_{ij}$ , since  $\mathbb{C}$  is an infinite integral domain. Therefore  $E(X)^t A E(X) = A$ , and the result follows on applying  $\psi_n$ .  $\square$

In fact we can avoid the use of 2.3.3. An alternative approach is presented in 3.1.

Let  $K$  be an algebraically closed field of characteristic  $p > 2$ . We now introduce the Chevalley group  $G(K)$  corresponding to  $L$ . We require the following notation: Let  $F = \mathbb{C}$  or  $K$ , and define

$$Sp(2l, F) = \{T \in GL(2l, F) : T^t A T = A\},$$

where  $A$  is given on p.59. We call  $Sp(2l, F)$  the *symplectic group* (over  $F$ ). It can be shown that each  $T \in Sp(2l, F)$  has determinant 1 (see [C1,1.3]), and so  $Sp(2l, F) \subseteq SL(2l, F)$ . Now, as in type  $A_l$ , the set  $\{h_{\alpha_i}, e_{\alpha} : \alpha_i \in \Delta, \alpha \in \Phi\}$  is a Chevalley basis of  $L$ . In the notation of 2.1 we have, for  $\Delta = \{\alpha_1, \dots, \alpha_{l-1}, \alpha_l\}$ ,  $t_i \in K$ ,

$$(*) \quad \begin{aligned} x_{\alpha_i}(t_i) &= \bar{I} + t_i(\bar{e}_{i,i+1} - \bar{e}_{(i+1)',i'}), \quad 1 \leq i \leq l-1, \\ x_{\alpha_l}(t_l) &= \bar{I} + t_l \bar{e}_{l,l'}. \end{aligned}$$

If  $\alpha \in \Phi^+ - \Delta$  then  $x_{\alpha}(t_{\alpha}) = \bar{I} + t_{\alpha} \bar{e}_{\alpha}$ , where  $2 \leq \text{ht}(\bar{e}_{\alpha}) \leq 2l-1$ ,  $e_{\alpha}$  running through the positive compound root vectors of  $L$ . It is shown in [R] that  $G(K) = Sp(2l, K)$ ; it is the simply-connected simple algebraic group of type  $C_l$  defined over  $K$ . Write  $G = G(K)$  for brevity. In this case, the subgroups of  $G$  as defined in (CG1) of 2.1 are:

$$U = Sp(2l, K) \cap U(2l, K), \quad T = Sp(2l, K) \cap D(2l, K), \quad \text{and} \quad B = Sp(2l, K) \cap B(2l, K).$$

For a more direct account of the group  $Sp(2l, K)$ , consult [DM,15.2].

The following result is well-known (refer to 2.2 for notation):

**Lemma 2.3.4** *Let  $u \in U = Sp(2l, K) \cap U(2l, K)$ , then the following hold:*

- (i)  $u(1) = (\mu_1, \mu_2, \dots, \mu_{l-1}, \mu_l, -\mu_{l-1}, \dots, -\mu_2, -\mu_1)$ , for some  $\mu_i \in K$ ,  $1 \leq i \leq l$ .
- (ii)  $u$  is regular  $\Leftrightarrow \mu_i \neq 0$  for all  $i = 1, 2, \dots, l$ .



**Proof** Argue as in the proof of 2.2.3, using (\*) above. □

We now come to the main result of this section. As in 2.2, the notation used in the proof is taken from 1.7.

**Theorem 2.3.5** *Let  $G = Sp(2l, K)$ ,  $l \geq 3$ , where  $K$  is an algebraically closed field of characteristic  $p > 2$ . Suppose  $u \in G_u$  is a regular unipotent element. Then the following hold:*

$$(i) \quad o(u) = p^t = \min\{p^s : s \in \mathbb{N} \text{ and } p^s > \text{ht}(r_0)\}.$$

(ii) *There exists a closed subgroup  $V$  of  $G$ , with  $V \cong W_t(K)$  and  $u \in V$ .*

**Proof** Let  $N = \sum_{\text{ht}(\alpha)=1} e_\alpha \in L = sp(2l, \mathbb{C})$ . Then  $0 \neq N$  is nilpotent, with  $p\text{-nilp}(N) = t \in \mathbb{N}$ , where by 2.3.2,

$$p^{t-1} \leq 2l - 1 = \text{ht}(r_0) \quad \text{and} \quad p^t > 2l - 1.$$

In the notation of 1.7, we have (for  $X = (X_0, X_1, \dots, X_{t-1})$ )

$$E(X) = \exp(d(X, N)) = \sum_{i=0}^{p^t-1} c(X)_i N^i \in M(2l, \mathbb{Z}_{(p)}[X]),$$

where  $c(X)_0 = 1$  and  $c(X)_1 = X_0$ . Let  $x = (x_0, x_1, \dots, x_{t-1}) \in W_t(\mathbb{C})$  be arbitrary. Substituting  $x_i$  for  $X_i$ ,  $0 \leq i \leq t-1$ , into  $d(X, N)$  gives  $d(x, N) = \sum_{i=0}^{t-1} d(x)_i N^{p^i}$ . Since  $p$  is odd, we have  $d(x, N) \in L$  by 2.3.1(i). It then follows from 2.3.1(ii) that

$$E(x) = \exp(d(x, N)) \in Sp(2l, \mathbb{C}) \cap U(2l, \mathbb{C}).$$

We now transfer to  $K$  (see (†) of 2.2). Write  $\bar{N} = \psi_{2l}(N)$ . By 2.2.1(b), we have  $p\text{-nilp}(\bar{N}) = p\text{-nilp}(N) = t$  (or use 2.3.2). Now

$$\bar{E}(X) = \psi_{2l}(E(X)) = \sum_{i=0}^{p^t-1} \bar{c}(X)_i \bar{N}^i \in M(2l, K[X]).$$

Fix  $y = (y_0, y_1, \dots, y_{t-1}) \in W_t(K)$ . Substituting  $y_i$  for  $X_i$ ,  $0 \leq i \leq t-1$ , in  $\bar{E}(X)$  gives

$$\bar{E}(y) = e_p(\bar{N}, y) \in U = Sp(2l, K) \cap U(2l, K) \subseteq G = Sp(2l, K),$$

by 2.3.3. As in 2.2.4 we have

$$e_p(\overline{N}, y) = \overline{I} + y_0 \overline{N} + \sum_{i=2}^{p^t-1} \overline{c}(y)_i \overline{N}^i,$$

where  $1 = \text{ht}(\overline{N}) < \text{ht}(\overline{N}^i)$ ,  $2 \leq i \leq p^t - 1$ . The description of  $N$  then makes it clear that

$$e_p(\overline{N}, y)(1) = (\underbrace{y_0, \dots, y_0}_{l-1 \text{ terms}}, y_0, \underbrace{-y_0, \dots, -y_0}_{l-1 \text{ terms}}).$$

Therefore, by 2.3.4, we have

$$\begin{aligned} e_p(\overline{N}, y) \text{ regular} &\Leftrightarrow y_0 \neq 0 \\ &\Leftrightarrow \text{o}(y) = p^t \quad (\text{by 1.2.3(c)}) \end{aligned} .$$

The argument now concludes as in 2.2.4. □

## 2.4 Type $B_l$

Let  $L = so(2l + 1, \mathbb{C})$ ,  $l \geq 2$ , be the set of all  $(2l + 1) \times (2l + 1)$  matrices  $x$  over  $\mathbb{C}$  satisfying

$$x^t A = -Ax,$$

where

$$A = \left( \begin{array}{ccc|c|ccc} & & & 0 & & & \\ & & & \vdots & & & \\ & 0 & & 0 & & J_l & \\ \hline 0 & \dots & 0 & 2 & 0 & \dots & 0 \\ \hline & & & 0 & & & \\ & J_l & & \vdots & & & \\ & & & 0 & & 0 & \end{array} \right), \quad J_l = \begin{pmatrix} 0 & & 1 \\ & \ddots & \\ 1 & & 0 \end{pmatrix}.$$

Then  $L$  is the complex simple Lie algebra of type  $B_l$  (consult the references in 2.2). Let  $H$  be the set of all  $(2l + 1) \times (2l + 1)$  diagonal matrices in  $L$ . Then  $H$  is a Cartan subalgebra of  $L$  (of  $l$  dimensions). The elements of  $H$  have the form

$$h = \begin{pmatrix} \lambda_1 & & & & & & \\ & \ddots & & & & & \\ & & \lambda_l & & & & \\ & & & 0 & & & \\ & & & & -\lambda_l & & \\ & & & & & \ddots & \\ & & & & & & -\lambda_1 \end{pmatrix}.$$

We will number the rows and columns of the matrices as follows:

$$1, 2, \dots, l-1, l, 0, l', (l-1)', \dots, 2', 1'.$$

The following conversion is clear: The label 0 represents the  $(l + 1)$ -th row or column of a given matrix. Now let  $1 \leq i \leq l$ , and consider the label  $i'$ . Then  $i'$  represents the  $(2l + 2 - i)$ -th row or column of a given matrix. Conversely the  $i$ -th row or column, where  $l + 2 \leq i \leq 2l + 1$ , is labelled by  $(2l + 2 - i)'$  in the new notation.

A basis for  $L$  is then

$$\begin{aligned}
h_i &= e_{ii} - e_{i'i'} , \quad 1 \leq i \leq l. \\
e_{\lambda_i - \lambda_j} &= e_{ij} - e_{j'i'} , \quad 1 \leq i < j \leq l. \\
e_{\lambda_j - \lambda_i} &= e_{ji} - e_{i'j'} , \quad 1 \leq i < j \leq l. \\
e_{\lambda_i + \lambda_j} &= e_{ij'} - e_{ji'} , \quad 1 \leq i < j \leq l. \\
e_{-\lambda_i - \lambda_j} &= e_{j'i} - e_{i'j} , \quad 1 \leq i < j \leq l. \\
e_{\lambda_i} &= 2e_{i0} - e_{0i'} , \quad 1 \leq i \leq l. \\
e_{-\lambda_i} &= e_{0i} - 2e_{i'0} , \quad 1 \leq i \leq l.
\end{aligned}$$

As in type  $C_l$  (see 2.3), the roots  $\Phi$  of  $L$  (relative to  $H$ ) will be identified with the various subscripts arising above. The elements

$$\alpha_1 = \lambda_1 - \lambda_2, \quad \alpha_2 = \lambda_2 - \lambda_3, \quad \dots, \quad \alpha_{l-1} = \lambda_{l-1} - \lambda_l, \quad \alpha_l = \lambda_l,$$

then form a set  $\Delta$  of simple roots of  $L$ . We partition the set  $\Phi^+$  of positive roots into the following three subsets:

$$\begin{aligned}
(1) \quad \Phi_{ij} &= \{\alpha_{ij} = \lambda_i - \lambda_j : 1 \leq i < j \leq l\} \\
(2) \quad \Phi_{ij'} &= \{\alpha_{ij'} = \lambda_i + \lambda_j : 1 \leq i < j \leq l\} \quad . \\
(3) \quad \Phi_{i0} &= \{\alpha_{i0} = \lambda_i : 1 \leq i \leq l\}
\end{aligned}$$

We have

$$\begin{aligned}
(1) \quad \text{ht}(\alpha_{ij}) &= j - i & ; \quad |\Phi_{ij}| &= l(l-1)/2 \\
(2) \quad \text{ht}(\alpha_{ij'}) &= 2l + 2 - j - i & ; \quad |\Phi_{ij'}| &= l(l-1)/2 \quad . \\
(3) \quad \text{ht}(\alpha_{i0}) &= l + 1 - i & ; \quad |\Phi_{i0}| &= l
\end{aligned}$$

For each  $\alpha \in \Phi^+$ , we have  $\text{ht}(e_\alpha) = \text{ht}(\alpha)$ , the root vectors corresponding to the simple roots being of height 1. The total number of positive roots is  $l^2$ . The highest root is

$$r_0 = \alpha_{12'} = \alpha_1 + 2\alpha_2 + \dots + 2\alpha_l,$$

of height  $\text{ht}(r_0) = 2l - 1$ .

As in case  $C_l$ , we list below the positive root vectors of odd height. Let  $r = 2s + 1$  where  $0 \leq s \leq l - 1$  (so that  $1 \leq r \leq 2l - 1$ ). The root vectors will be partitioned into the three subsets defined above.

Case (i)

$$\text{Suppose } 1 \leq r \leq \begin{cases} l-2 & : l \text{ odd} \\ l-1 & : l \text{ even} \end{cases}.$$

$$(1) \quad e_{\alpha_{ij}} = e_{ij} - e_{j'i'}, \quad j = i + r,$$

where  $1 \leq i \leq l - r$ . There are  $l - r = l - 2s - 1$  root vectors of this form.

$$(2) \quad e_{\alpha_{ij'}} = e_{ij'} - e_{ji'}, \quad j = 2l + 2 - (i + r),$$

where  $l + 1 - 2s \leq i \leq l - s$ , and  $s \neq 0$ . There are  $s$  root vectors of this form.

$$(3) \quad e_{\alpha_{i0}} = 2e_{i0} - e_{0i'},$$

where  $i = l - 2s$ . There is 1 root vector of this form.

Case (ii)

$$\text{Suppose } \begin{cases} l \leq r \leq 2l - 1 & : l \text{ odd} \\ l + 1 \leq r \leq 2l - 1 & : l \text{ even} \end{cases}.$$

(1) There is no contribution from this subset.

$$(2) \quad e_{\alpha_{ij'}} = e_{ij'} - e_{ji'}, \quad j = 2l + 2 - (i + r),$$

where  $1 \leq i \leq l - s$  provided  $r \neq l$ , and  $2 \leq i \leq l - s$  if  $r = l$  (is odd). There are  $l - s$  root vectors of this form provided  $r \neq l$ , and  $l - s - 1$  if  $r = l$ .

$$(3) \quad e_{\alpha_{10}} = 2e_{10} - e_{01'},$$

only when  $r = l$  (is odd).

We give below the analogue of 2.2.2 for the case  $B_l$ :

**Lemma 2.4.1** *Let*

$$N = \sum_{\text{ht}(\alpha)=1} e_{\alpha} = e_{\alpha_1} + \cdots + e_{\alpha_{l-1}} + e_{\alpha_l} \in L = \mathfrak{so}(2l + 1, \mathbb{C}), \quad l \geq 2.$$

*Then the following hold:*

(a) *Let  $r = 2s + 1$  where  $0 \leq s \leq l - 1$ .*

Case (i)

Suppose  $1 \leq r \leq \begin{cases} l-2 & : l \text{ odd} \\ l-1 & : l \text{ even} \end{cases}$ , then

$$N = \sum_{i=1}^{l-1} e_{\alpha_{i,i+1}} + e_{\alpha_{l,0}},$$

$$N^r = \sum_{i=1}^{l-r} e_{\alpha_{i,i+r}} + 2(-1)^l \sum_{i=l+1-2s}^{l-s} (-1)^i e_{\alpha_{i,(2l+2-i-r)'}} + e_{\alpha_{l-2s,0}}, \quad s \neq 0.$$

Case (ii)

Suppose  $\begin{cases} l \leq r \leq 2l-1 & : l \text{ odd} \\ l+1 \leq r \leq 2l-1 & : l \text{ even} \end{cases}$ , then

$$N^l = -2 \sum_{i=2}^{(l+1)/2} (-1)^i e_{\alpha_{i,(l+2-i)'}} + e_{\alpha_{1,0}}, \quad l \text{ odd},$$

$$N^r = 2(-1)^l \sum_{i=1}^{l-s} (-1)^i e_{\alpha_{i,(2l+2-i-r)'}} \quad , \quad r \neq l.$$

In particular, in both cases,  $N^r = \sum_{\text{ht}(\alpha)=r} \lambda_\alpha e_\alpha$ , where each  $\lambda_\alpha \in \{-2, -1, 1, 2\}$  depends on  $l$ ,  $s$ , and  $\alpha$ , and  $N^{\text{ht}(r_0)} = 2(-1)^{l-1} e_{r_0}$ .

(b)  $N^i = 0$  for  $i \geq 2l+1$  (and  $0 \neq N^{2l} = 2(-1)^l e_{1,1'} \notin L$ ).

**Proof** In the ‘old’ notation we have

$$N = \sum_{i=1}^{2l} \lambda_i e_{i,i+1} \quad \text{where} \quad \lambda_i = \begin{cases} 1 & : 1 \leq i \leq l-1 \\ 2 & : i = l \\ -1 & : l+1 \leq i \leq 2l \end{cases}.$$

The argument now proceeds as in the proof of 2.3.2, using the description of the root vectors of odd height given above.  $\square$

Let  $K$  be an algebraically closed field of characteristic  $p > 2$ . We now introduce the Chevalley group  $G(K)$  corresponding to  $L$ . We require the following notation: Let  $F = \mathbb{C}$  or  $K$ , and define

$$O(2l+1, F) = \{T \in GL(2l+1, F) : T^t A T = A\},$$

where  $A$  is given on p.67. Let  $T \in O(2l+1, F)$ , then since  $\det(A) = 2(-1)^l \neq 0$ , we have  $\det(T) = \pm 1$ . Define

$$SO(2l+1, F) = O(2l+1, F) \cap SL(2l+1, F),$$

the *special orthogonal group* (over  $F$ ); a normal subgroup of  $O(2l+1, F)$  of index 2. Now the set  $\{h_{\alpha_i}, e_{\alpha} : \alpha_i \in \Delta, \alpha \in \Phi\}$  is a Chevalley basis of  $L$ . In the notation of 2.1 we have, for  $\Delta = \{\alpha_1, \dots, \alpha_{l-1}, \alpha_l\}$ ,  $t_i \in K$ ,

$$(*) \quad \begin{aligned} x_{\alpha_i}(t_i) &= \bar{I} + t_i(\bar{e}_{i,i+1} - \bar{e}_{(i+1)',i'}), \quad 1 \leq i \leq l-1, \\ x_{\alpha_l}(t_l) &= \bar{I} + t_l(2\bar{e}_{l,0} - \bar{e}_{0,l'}) - t_l^2 \bar{e}_{l,l'}. \end{aligned}$$

If  $\alpha \in \Phi^+ - \Delta$  then  $2 \leq \text{ht}(x_{\alpha}(t_{\alpha}) - \bar{I}) \leq 2l-1$ , where  $t_{\alpha} \in K$ . It is shown in [R] that  $G(K) = \Omega(2l+1, K)$ , the commutator subgroup of  $O(2l+1, K)$ . Now  $\Omega(2l+1, K) \subseteq SO(2l+1, K)$  - in fact equals the commutator subgroup of  $SO(2l+1, K)$  - and

$$\frac{SO(2l+1, K)}{\Omega(2l+1, K)} \cong \frac{K^*}{(K^*)^2}$$

(see [Di,II,8]). Since  $K$  is algebraically closed, we obtain  $G(K) = SO(2l+1, K)$ ; it is the *adjoint* simple algebraic group of type  $B_l$  defined over  $K$ . Write  $G = G(K)$  for brevity. In this case, the subgroups of  $G$  as defined in (CG1) of 2.1 are:

$$U = SO(2l+1, K) \cap U(2l+1, K), \quad T = SO(2l+1, K) \cap D(2l+1, K),$$

$$\text{and } B = SO(2l+1, K) \cap B(2l+1, K).$$

The following result is well-known:

**Lemma 2.4.2** *Let  $u \in U = SO(2l+1, K) \cap U(2l+1, K)$ , then the following hold:*

- (i)  $u(1) = (\mu_1, \mu_2, \dots, \mu_{l-1}, 2\mu_l, -\mu_l, -\mu_{l-1}, \dots, -\mu_2, -\mu_1)$ , with  $\mu_i \in K$ ,  $1 \leq i \leq l$ .
- (ii)  $u$  is regular  $\Leftrightarrow \mu_i \neq 0$  for all  $i = 1, 2, \dots, l$ .

**Proof** Argue as in the proof of 2.2.3, using (\*) above. □

We now come to the main result of this section.

**Theorem 2.4.3** *Let  $G = SO(2l + 1, K)$ ,  $l \geq 2$ , where  $K$  is an algebraically closed field of characteristic  $p > 2$ . Suppose  $u \in G_u$  is a regular unipotent element. Then the following hold:*

(i)  $o(u) = p^t = \min\{p^s : s \in \mathbb{N} \text{ and } p^s > \text{ht}(r_0)\}$ .

(ii) *There exists a closed subgroup  $V$  of  $G$ , with  $V \cong W_t(K)$  and  $u \in V$ .*

**Proof** Argue as in the proof of 2.3.5, using 2.4.1 and 2.4.2. □



## 2.5 Type $D_l$

Let  $L = so(2l, \mathbb{C})$ ,  $l \geq 4$ , be the set of all  $(2l) \times (2l)$  matrices  $x$  over  $\mathbb{C}$  satisfying

$$x^t A = -Ax,$$

where

$$A = \left( \begin{array}{c|c} 0 & J_l \\ \hline J_l & 0 \end{array} \right) \quad , \quad J_l = \begin{pmatrix} 0 & & 1 \\ & \ddots & \\ 1 & & 0 \end{pmatrix} .$$

Then  $L$  is the complex simple Lie algebra of type  $D_l$  (consult the references in 2.2). Let  $H$  be the set of all  $(2l) \times (2l)$  diagonal matrices in  $L$ . Then  $H$  is a Cartan subalgebra of  $L$  (of  $l$  dimensions). The elements of  $H$  have the form

$$h = \begin{pmatrix} \lambda_1 & & & & & \\ & \ddots & & & & \\ & & \lambda_l & & & \\ & & & -\lambda_l & & \\ & & & & \ddots & \\ & & & & & -\lambda_1 \end{pmatrix} .$$

We will number the rows and columns of the matrices as follows (see 2.3):

$$1, \ 2, \ \dots, \ l-1, \ l, \ l', \ (l-1)', \ \dots, \ 2', \ 1'.$$

A basis for  $L$  is then

$$\begin{aligned} h_i &= e_{ii} - e_{i'i'} , \quad 1 \leq i \leq l. \\ e_{\lambda_i - \lambda_j} &= e_{ij} - e_{j'i'} , \quad 1 \leq i < j \leq l. \\ e_{\lambda_j - \lambda_i} &= e_{ji} - e_{i'j'} , \quad 1 \leq i < j \leq l. \\ e_{\lambda_i + \lambda_j} &= e_{ij'} - e_{ji'} , \quad 1 \leq i < j \leq l. \\ e_{-\lambda_i - \lambda_j} &= e_{j'i} - e_{i'j} , \quad 1 \leq i < j \leq l. \end{aligned}$$

As in type  $C_l$  (see 2.3), the roots  $\Phi$  of  $L$  (relative to  $H$ ) will be identified with the various subscripts arising above. The elements

$$\alpha_1 = \lambda_1 - \lambda_2, \quad \alpha_2 = \lambda_2 - \lambda_3, \quad \dots, \quad \alpha_{l-1} = \lambda_{l-1} - \lambda_l, \quad \alpha_l = \lambda_{l-1} + \lambda_l ,$$

then form a set  $\Delta$  of simple roots of  $L$ . We partition the set  $\Phi^+$  of positive roots into the following two subsets:

$$(1) \quad \Phi_{ij} = \{\alpha_{ij} = \lambda_i - \lambda_j : 1 \leq i < j \leq l\}$$

$$(2) \quad \Phi_{ij'} = \{\alpha_{ij'} = \lambda_i + \lambda_j : 1 \leq i < j \leq l\}$$

We have

$$(1) \quad \text{ht}(\alpha_{ij}) = j - i \quad ; \quad |\Phi_{ij}| = l(l-1)/2$$

$$(2) \quad \text{ht}(\alpha_{ij'}) = 2l - j - i \quad ; \quad |\Phi_{ij'}| = l(l-1)/2$$

Let  $\alpha = \alpha_{ij} \in \Phi_{ij}$ , then  $\text{ht}(e_\alpha) = \text{ht}(\alpha)$ . However if  $\alpha = \alpha_{ij'} \in \Phi_{ij'}$ , then  $\text{ht}(e_\alpha) = \text{ht}(\alpha) + 1$ . This is a consequence of the fact that  $\text{ht}(e_{\alpha_l}) = 2$ , whereas the root vectors corresponding to the simple roots in  $\Phi_{ij}$  are of height 1. The total number of positive roots is  $l(l-1)$ . The highest root is

$$r_0 = \alpha_{12'} = \alpha_1 + 2\alpha_2 + \cdots + 2\alpha_{l-2} + \alpha_{l-1} + \alpha_l,$$

of height  $\text{ht}(r_0) = 2l - 3$ .

For convenience we list below the positive roots of odd height: Let  $r = 2s + 1$  where  $1 \leq s \leq l - 2$  (so that  $3 \leq r \leq 2l - 3$ ). The roots will be partitioned into the two subsets defined above.

Case (i)

$$\text{Suppose } 3 \leq r \leq \begin{cases} l - 2 & : l \text{ odd} \\ l - 1 & : l \text{ even} \end{cases}.$$

$$(1) \quad \alpha_{ij}, \quad j = i + r,$$

where  $1 \leq i \leq l - r$ . There are  $l - r = l - 2s - 1$  roots of this form.

$$(2) \quad \alpha_{ij'}, \quad j = 2l - (i + r),$$

where  $l - 2s - 1 \leq i \leq l - s - 1$ . There are  $s + 1$  roots of this form.

Case (ii)

$$\text{Suppose } \begin{cases} l \leq r \leq 2l - 3 & : l \text{ odd} \\ l + 1 \leq r \leq 2l - 3 & : l \text{ even} \end{cases}.$$

(1) There is no contribution from this subset.

$$(2) \quad \alpha_{ij'}, \quad j = 2l - (i + r),$$

where  $1 \leq i \leq l - s - 1$ . There are  $l - s - 1$  roots of this form.

The analogue of 2.2.2 for the case  $D_l$  follows from the next result. For the purposes of this lemma, we revert to the (old) notation of numbering rows and columns by  $1, 2, \dots, l, l + 1, \dots, 2l - 1, 2l$ .

**Lemma 2.5.1** *Let*

$$N = \sum_{i=1}^{l-1} e_{i,i+1} - \sum_{i=l+1}^{2l-1} e_{i,i+1} + e_{l-1,l+1} - e_{l,l+2} \in M(2l, \mathbb{C}), \quad l \geq 4.$$

*Then the following hold:*

(i) *If  $2 \leq r \leq l - 1$  then*

$$N^r = \sum_{i=1}^{l-r} e_{i,i+r} + (-1)^r \sum_{i=l+1}^{2l-r} e_{i,i+r} + e_{l-r,l+1} + (-1)^r e_{l,l+r+1} + 2(-1)^{l-r} \sum_{i=l+1-r}^{l-1} (-1)^i e_{i,i+r+1}.$$

(ii) *If  $l \leq r \leq 2l - 2$  then*

$$N^r = 2(-1)^{r-l} \sum_{i=1}^{2l-r-1} (-1)^i e_{i,i+r+1}.$$

(iii)  $N^r = 0, \quad r \geq 2l - 1$ .

**Proof** The result is clearly true for  $r = 1$ , so assume  $r \geq 2$ , and that the result holds for  $r - 1$ . Recall

$$(*) \quad e_{ij} e_{i'j'} = \delta_{ji'} e_{ij'}, \quad 1 \leq i, j, i', j' \leq 2l.$$

There are various cases to consider: If  $r - 1 \geq 2l - 1$  then  $N^{r-1} = 0$  (by (iii)), and so  $N^r = 0$ . If  $r - 1 = 2l - 2$  then  $N^{r-1} = 2(-1)^{l-1} e_{1,2l}$  (by (ii)), and so  $N^r = N N^{r-1} = 0$  by (\*). Now suppose  $l \leq r - 1 \leq 2l - 3$ , so that  $N^{r-1} = 2(-1)^{r-l-1} \sum_{i=1}^{2l-r} (-1)^i e_{i,i+r}$  (by (ii)). Note that the *largest* value of  $2l - r$  is  $2l - (l + 1) = l - 1$ . By (\*) we have

$$\begin{aligned} N^r = N N^{r-1} &= 2(-1)^{r-l-1} \left( \sum_{i=1}^{l-1} e_{i,i+1} \right) \left( \sum_{i=1}^{2l-r} (-1)^i e_{i,i+r} \right) \\ &= 2(-1)^{r-l} \sum_{i=1}^{2l-r-1} (-1)^i e_{i,i+r+1}. \end{aligned}$$

Next consider the case  $r - 1 = l - 1$ . By (i) we have

$$N^{r-1} = e_{1,l} + (-1)^{l-1} e_{l+1,2l} + e_{1,l+1} + (-1)^{l-1} e_{l,2l} - 2 \sum_{i=2}^{l-1} (-1)^i e_{i,i+l}.$$

Using (\*) and the description of  $N$ , we obtain

$$\begin{aligned} N^r &= N N^{r-1} \\ &= \left( \sum_{i=1}^{l-1} e_{i,i+1} + e_{l-1,l+1} \right) \left( (-1)^{l-1} e_{l+1,2l} + (-1)^{l-1} e_{l,2l} - 2 \sum_{i=2}^{l-1} (-1)^i e_{i,i+l} \right) \\ &= 2(-1)^{l-1} e_{l-1,2l} - 2 \left( \sum_{i=1}^{l-1} e_{i,i+1} \right) \left( \sum_{i=2}^{l-1} (-1)^i e_{i,i+l} \right) \\ &= 2 \sum_{i=1}^{l-1} (-1)^i e_{i,i+l+1}. \end{aligned}$$

Now suppose  $2 \leq r - 1 \leq l - 2$ , so that (i) gives

$$\begin{aligned} N^{r-1} &= \sum_{i=1}^{l-r+1} e_{i,i+r-1} + (-1)^{r-1} \sum_{i=l+1}^{2l-r+1} e_{i,i+r-1} + e_{l-r+1,l+1} \\ &\quad + (-1)^{r-1} e_{l,l+r} + 2(-1)^{l-r+1} \sum_{i=l+2-r}^{l-1} (-1)^i e_{i,i+r}. \end{aligned}$$

Note that  $2 \leq l - r + 1 \leq l - 2$ . Using (\*) and the description of  $N$ , we obtain

$$\begin{aligned} N^r &= N N^{r-1} \\ &= \left( \sum_{i=1}^{l-1} e_{i,i+1} \right) \left( \sum_{i=1}^{l-r+1} e_{i,i+r-1} \right) + (-1)^r \left( \sum_{i=l+1}^{2l-1} e_{i,i+1} \right) \left( \sum_{i=l+1}^{2l-r+1} e_{i,i+r-1} \right) + 2(-1)^{r-1} e_{l-1,l+r} \\ &\quad + (-1)^r e_{l,l+r+1} + e_{l-r,l+1} + 2(-1)^{l-r+1} \left( \sum_{i=1}^{l-1} e_{i,i+1} \right) \left( \sum_{i=l+2-r}^{l-1} (-1)^i e_{i,i+r} \right) \\ &= \sum_{i=1}^{l-r} e_{i,i+r} + (-1)^r \sum_{i=l+1}^{2l-r} e_{i,i+r} + e_{l-r,l+1} + (-1)^r e_{l,l+r+1} + 2(-1)^{l-r} \sum_{i=l+1-r}^{l-1} (-1)^i e_{i,i+r+1}. \end{aligned}$$

This leaves the case  $r - 1 = 1$ , which follows in a similar way. Therefore in each case,  $N^r$  is of the desired form.  $\square$

As a direct consequence we have the following

**Corollary 2.5.2** *Let*

$$N = \sum_{\text{ht}(\alpha)=1} e_{\alpha} = e_{\alpha_1} + \cdots + e_{\alpha_{l-1}} + e_{\alpha_l} \in L = \mathfrak{so}(2l, \mathbb{C}), \quad l \geq 4.$$

*Then the following hold:*

(a) Let  $r = 2s + 1$  where  $1 \leq s \leq l - 2$ .

Case (i)

Suppose  $3 \leq r \leq \begin{cases} l - 2 & : l \text{ odd} \\ l - 1 & : l \text{ even} \end{cases}$ , then

$$N^r = \sum_{i=1}^{l-r} e_{\alpha_{i,i+r}} + e_{\alpha_{l-r,l'}} + 2(-1)^{l-1} \sum_{i=l-2s}^{l-s-1} (-1)^i e_{\alpha_{i,(2l-i-r)'}}.$$

Case (ii)

Suppose  $\begin{cases} l \leq r \leq 2l - 3 & : l \text{ odd} \\ l + 1 \leq r \leq 2l - 3 & : l \text{ even} \end{cases}$ , then

$$N^r = 2(-1)^{l-1} \sum_{i=1}^{l-s-1} (-1)^i e_{\alpha_{i,(2l-i-r)'}}.$$

In particular, in both cases,  $N^r = \sum_{\text{ht}(\alpha)=r} \lambda_\alpha e_\alpha$ , where each  $\lambda_\alpha \in \{-2, -1, 1, 2\}$  depends on  $l, s$ , and  $\alpha$ , and  $N^{\text{ht}(r_0)} = 2(-1)^l e_{r_0}$ .

(b)  $N^i = 0$  for  $i \geq 2l - 1$  (and  $0 \neq N^{2l-2} = 2(-1)^{l-1} e_{1,1'} \notin L$ ).

**Proof** We only prove part (a)(ii), with part(a)(i) and (b) following in a similar way. Note the following (obvious) property of finite sequences:

$$(**) \quad \sum_{i=1}^t a_i = \sum_{i=1}^t a_{t+1-i}, \quad t \in \mathbb{N}.$$

By 2.5.1(ii) we have, since  $r$  is odd,

$$(-1)^{1-l} N^r / 2 = \sum_{i=1}^{l-s-1} (-1)^i e_{i,i+r+1} + \sum_{i=l-s}^{2(l-s-1)} (-1)^i e_{i,i+r+1},$$

where

$$\sum_{i=l-s}^{2(l-s-1)} (-1)^i e_{i,i+r+1} = \sum_{i=1}^{l-s-1} (-1)^{i-1+l-s} e_{i-1+l-s, i+l+s+1} = - \sum_{i=1}^{l-s-1} (-1)^i e_{2l-i-r, 2l-i+1},$$

using (\*\*). Numbering rows and columns as on p.73, then gives

$$(-1)^{1-l} N^r / 2 = \sum_{i=1}^{l-s-1} (-1)^i (e_{i,(2l-i-r)'} - e_{2l-i-r,i'}) = \sum_{i=1}^{l-s-1} (-1)^i e_{\alpha_{i,(2l-i-r)'}}$$

(see p.74, the summation involving *all* roots of height  $r$ ).

□

Let  $K$  be an algebraically closed field of characteristic  $p > 2$ . We now introduce the Chevalley group  $G(K)$  corresponding to  $L$ . We require the following notation: Let  $F = \mathbb{C}$  or  $K$ , and define (as in 2.4)  $O(2l, F) = \{T \in GL(2l, F) : T^t A T = A\}$ , where  $A$  is given on p.73, and  $SO(2l, F) = O(2l, F) \cap SL(2l, F)$ . Now the set  $\{h_{\alpha_i}, e_{\alpha} : \alpha_i \in \Delta, \alpha \in \Phi\}$  is a Chevalley basis of  $L$ . In the notation of 2.1 we have, for  $\Delta = \{\alpha_1, \dots, \alpha_{l-1}, \alpha_l\}$ ,  $t_i \in K$ ,

$$(*_1) \quad \begin{aligned} x_{\alpha_i}(t_i) &= \bar{I} + t_i(\bar{e}_{i,i+1} - \bar{e}_{(i+1)',i'}), \quad 1 \leq i \leq l-1 \\ x_{\alpha_l}(t_l) &= \bar{I} + t_l(\bar{e}_{l-1,l'} - \bar{e}_{l,(l-1)'}) \end{aligned}$$

We also list the height 2 elements corresponding to the roots  $\alpha \in \Phi_{ij}$  of height 2:

$$(*_2) \quad x_{\alpha_{i,i+2}}(t'_i) = \bar{I} + t'_i(\bar{e}_{i,i+2} - \bar{e}_{(i+2)',i'}), \quad t'_i \in K, \quad 1 \leq i \leq l-2.$$

The remaining  $\alpha \in \Phi^+ - \Delta$  satisfy  $3 \leq \text{ht}(x_{\alpha}(t_{\alpha}) - \bar{I}) \leq 2l-2$ , where  $t_{\alpha} \in K$ . It is shown in [R] that  $G(K) = \Omega(2l, K) = SO(2l, K)$  (compare with 2.4); it is a simple algebraic group of type  $D_l$  defined over  $K$ , neither simply-connected nor adjoint. Write  $G = G(K)$  for brevity. In this case, the subgroups of  $G$  as defined in (CG1) of 2.1 are:

$$U = SO(2l, K) \cap U(2l, K), \quad T = SO(2l, K) \cap D(2l, K), \quad \text{and} \quad B = SO(2l, K) \cap B(2l, K).$$

For a more direct account of the group  $SO(2l, K)$ , consult [DM,15.3].

Let  $u = (u_{ij}) \in U(2l, K)$ ,  $1 \leq i, j \leq 2l$ . In 2.2 we defined  $u(1) = (u_{12}, u_{23}, \dots, u_{2l-1,2l})$ . Now define  $u(2) = (u_{13}, u_{24}, \dots, u_{2l-2,2l})$ ; that is, the 'vector' of height 2 elements of  $u$ . The following result is well-known:

**Lemma 2.5.3** *Let  $u \in U = SO(2l, K) \cap U(2l, K)$ , then the following hold:*

- (i)  $u(1) = (\mu_1, \mu_2, \dots, \mu_{l-1}, 0, -\mu_{l-1}, \dots, -\mu_2, -\mu_1)$ , for some  $\mu_i \in K$ ,  $1 \leq i \leq l-1$ , and  $u(2)$  is of the form:

$$u(2) = (\underbrace{*, \dots, *}_{l-2 \text{ terms}}, \mu_l, -\mu_l, \underbrace{*, \dots, *}_{l-2 \text{ terms}}),$$

where  $\mu_i \in K$  (the various  $*$  do not concern us).

- (ii)  $u$  is regular  $\Leftrightarrow \mu_i \neq 0$  for all  $i = 1, 2, \dots, l$ .

**Proof** Argue as in the proof of 2.2.3, using  $(*_1)$  and  $(*_2)$  above.

We now come to the main result of this section.

**Theorem 2.5.4** *Let  $G = SO(2l, K)$ ,  $l \geq 4$ , where  $K$  is an algebraically closed field of characteristic  $p > 2$ . Suppose  $u \in G_u$  is a regular unipotent element. Then the following hold:*

(i)  $o(u) = p^t = \min\{p^s : s \in \mathbb{N} \text{ and } p^s > \text{ht}(r_0)\}$ .

(ii) *There exists a closed subgroup  $V$  of  $G$ , with  $V \cong W_t(K)$  and  $u \in V$ .*

**Proof** Let  $N = \sum_{\text{ht}(\alpha)=1} e_\alpha \in L = \mathfrak{so}(2l, \mathbb{C})$ . Then since  $p > 2$ , we have  $p\text{-nilp}(\overline{N}) = p\text{-nilp}(N) = t \in \mathbb{N}$ , where  $p^{t-1} \leq 2l - 3 = \text{ht}(r_0)$  and  $p^t > 2l - 3$  (see 2.5.2). Now argue as in the proof of 2.3.5, using 2.5.1, 2.5.2, and 2.5.3.  $\square$

## 2.6 Type $G_2$

We begin this section with a brief account of the complex simple Lie algebra of type  $G_2$ . For more details, consult [Sc,III,8] and [Se1,6]. Let  $F = \mathbb{C}$  or  $K$ , an algebraically closed field of characteristic  $p > 0$ ,  $p \neq 2$ . Write  $V = F^3$  and let

$$v \cdot w \quad \text{and} \quad v \times w$$

denote, respectively, the usual scalar and vector products of the vectors  $v, w \in V$ . Let  $e_1 = (1, 0, 0)$ ,  $e_2 = (0, 1, 0)$ , and  $e_3 = (0, 0, 1)$  be the standard basis for  $V$ . We have

$$e_i \cdot e_i = 1, \quad i = 1, 2, 3, \quad \text{and} \quad e_i \cdot e_j = 0, \quad i \neq j = 1, 2, 3,$$

$$e_1 \times e_2 = e_3, \quad e_2 \times e_3 = e_1, \quad \text{and} \quad e_3 \times e_1 = e_2.$$

We can now define the *split exceptional Cayley algebra*  $\mathcal{C}(F)$ . As a set  $\mathcal{C}(F)$  consists of all  $2 \times 2$  matrices of the form

$$\begin{pmatrix} \alpha & v \\ w & \beta \end{pmatrix},$$

where  $\alpha, \beta \in F$ ,  $v, w \in V$ . Addition and scalar multiplication are defined in the usual way for matrices. The algebra multiplication in  $\mathcal{C}(F)$ , denoted by juxtaposition, is defined as follows:

$$\begin{pmatrix} \alpha & v \\ w & \beta \end{pmatrix} \begin{pmatrix} \alpha' & v' \\ w' & \beta' \end{pmatrix} = \begin{pmatrix} \alpha\alpha' + v \cdot w' & \alpha v' + \beta' v - w \times w' \\ \alpha' w + \beta w' + v \times v' & \beta\beta' + w \cdot v' \end{pmatrix},$$

where  $\alpha, \alpha', \beta, \beta' \in F$ ,  $v, v', w, w' \in V$ . This gives  $\mathcal{C}(F)$  the structure of an 8-dimensional *alternative algebra* (that is,  $(x^2)y = x(xy)$  and  $y(x^2) = (yx)x$  for all  $x, y \in \mathcal{C}(F)$ ). We fix a basis  $\beta = \{c_1, c_2, \dots, c_8\}$ , where

$$c_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad c_2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \quad c_{2+i} = \begin{pmatrix} 0 & e_i \\ 0 & 0 \end{pmatrix}, \quad c_{5+i} = \begin{pmatrix} 0 & 0 \\ e_i & 0 \end{pmatrix},$$

$1 \leq i \leq 3$ . Write  $1 = c_1 + c_2$ , then  $x1 = 1x = x$  for all  $x \in \mathcal{C}(F)$ , and so 1 is the *identity element* in  $\mathcal{C}(F)$ .



The multiplication table for  $\beta$ , and hence for  $\mathcal{C}(F)$ , is given below:

	$c_1$	$c_2$	$c_3$	$c_4$	$c_5$	$c_6$	$c_7$	$c_8$
$c_1$	$c_1$	0	$c_3$	$c_4$	$c_5$	0	0	0
$c_2$	0	$c_2$	0	0	0	$c_6$	$c_7$	$c_8$
$c_3$	0	$c_3$	0	$c_8$	$-c_7$	$c_1$	0	0
$c_4$	0	$c_4$	$-c_8$	0	$c_6$	0	$c_1$	0
$c_5$	0	$c_5$	$c_7$	$-c_6$	0	0	0	$c_1$
$c_6$	$c_6$	0	$c_2$	0	0	0	$-c_5$	$c_4$
$c_7$	$c_7$	0	0	$c_2$	0	$c_5$	0	$-c_3$
$c_8$	$c_8$	0	0	0	$c_2$	$-c_4$	$c_3$	0

For example,  $c_1 c_3 = c_3$ .

Given

$$x = \begin{pmatrix} \alpha & v \\ w & \beta \end{pmatrix} \in \mathcal{C}(F),$$

we shall define (as usual)  $\text{tr}(x) = \alpha + \beta \in F$ . Define  $\mathcal{C}(F)_0 = \{x \in \mathcal{C}(F) : \text{tr}(x) = 0\}$ . Then  $\mathcal{C}(F)_0$  is a vector subspace of  $\mathcal{C}(F)$ , with basis  $\beta' = \{c_1 - c_2, c_3, c_4, c_5, c_6, c_7, c_8\}$ . Moreover  $\mathcal{C}(F)_0 \cap F1 = 0$ , and so  $\mathcal{C}(F) = \mathcal{C}(F)_0 \oplus F1$ . Indeed

$$\begin{pmatrix} \alpha & v \\ w & \beta \end{pmatrix} = \begin{pmatrix} (\alpha - \beta)/2 & v \\ w & -(\alpha - \beta)/2 \end{pmatrix} + \frac{\alpha + \beta}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in \mathcal{C}(F)_0 + F1.$$

Let  $\mathcal{C}(F)'$  denote the subspace of  $\mathcal{C}(F)$  spanned by all commutators  $[x, y] = xy - yx$ ,  $x, y \in \mathcal{C}(F)$ . The multiplication in  $\mathcal{C}(F)$  makes it clear that  $\mathcal{C}(F)' \subseteq \mathcal{C}(F)_0$ . Now  $[c_5, c_8] = c_1 - c_2$ ,  $[c_1, c_i] = c_i$ , and  $[c_{i+3}, c_1] = c_{i+3}$ ,  $3 \leq i \leq 5$ , and so  $\mathcal{C}(F)' = \mathcal{C}(F)_0$ .

Let  $\mathcal{A}(F)$  be a non-associative algebra over  $F$ . An element  $\delta \in \text{End } \mathcal{A}(F)$  is called a *derivation* of  $\mathcal{A}(F)$  if the following condition is satisfied:

$$\delta(xy) = (\delta x)y + x(\delta y),$$

for all  $x, y \in \mathcal{A}(F)$ . Let  $\text{Der } \mathcal{A}(F)$  be the collection of all such derivations, a Lie algebra under commutation.

Now consider the case where  $F = \mathbb{C}$  (over which our Lie algebras are defined). Write  $\mathcal{C} = \mathcal{C}(\mathbb{C})$ ,  $\mathcal{C}_0 = \mathcal{C}(\mathbb{C})_0$ , and  $\mathcal{C}' = \mathcal{C}(\mathbb{C})'$ , for brevity. Define  $L = \text{Der } \mathcal{C}$ , then  $L$  is the complex simple Lie algebra of type  $G_2$ . If  $\Delta = \{\alpha_1, \alpha_2\}$  denotes the set of simple roots of  $L$ , then the set of positive roots is

$$\Phi^+ = \{\alpha_1, \alpha_2, \alpha_1 + \alpha_2, 2\alpha_1 + \alpha_2, 3\alpha_1 + \alpha_2, 3\alpha_1 + 2\alpha_2\}.$$

The highest root is  $r_0 = 3\alpha_1 + 2\alpha_2$ , of height  $\text{ht}(r_0) = 5$ .

We shall require the following notation. See [L,XIII,5] for more details. Let  $f \in E = \text{End } V$ , and define an element  $f^t \in E$  by

$$f^t(e_i) = (e_i \cdot f(e_1), e_i \cdot f(e_2), e_i \cdot f(e_3)), \quad 1 \leq i \leq 3,$$

and extend linearly. The map  $f^t$  is called the *transpose* of  $f$ , with respect to the scalar product  $\cdot$  on  $V$ . If  $M(g)$  denotes the matrix representing  $g \in E$  with respect to the basis  $\{e_1, e_2, e_3\}$  of  $V$ , then

$$M(f^t) = M(f)^t.$$

For  $1 \leq i, j \leq 3$  define  $E_{ij} \in E$  as follows:

$$E_{ij}(e_j) = e_i \quad \text{and} \quad E_{ij}(e_k) = 0, \quad k \neq j,$$

and extend linearly. It is clear that  $M(E_{ij}) = e_{ij}$ , and  $E_{ij}^t = E_{ji}$ . Finally, the elements  $f \in E$  of trace zero (that is,  $\text{tr}(M(f)) = 0$ ) form a Lie algebra of type  $A_2$ , which we also denote by  $A_2$ . We then have the following

**Lemma 2.6.1** [Se1,6] *The map*

$$\begin{aligned} \psi : V \oplus V \oplus A_2 &\rightarrow L \\ (v_1, v_2, f) &\mapsto \delta \end{aligned},$$

where

$$(*) \quad \delta \begin{pmatrix} \alpha & v \\ w & \beta \end{pmatrix} = \begin{pmatrix} -v \cdot v_2 - w \cdot v_1 & (\alpha - \beta)v_1 + v_2 \times w - f^t(v) \\ (\alpha - \beta)v_2 + v_1 \times v + f(w) & v \cdot v_2 + w \cdot v_1 \end{pmatrix},$$

is a vector space isomorphism.

From now on we shall write  $\delta = (v_1, v_2, f)$ , where  $v_1, v_2 \in V$ ,  $f \in A_2$ , to mean the element  $\delta \in L$  defined by  $(*)$  above. If  $\varepsilon = (\bar{v}_1, \bar{v}_2, \bar{f}) \in L$ , then  $[\delta, \varepsilon] = (w_1, w_2, g) \in L$ , where

$$\begin{aligned}
 w_1 &= 2v_2 \times \bar{v}_2 - f^t(\bar{v}_1) + \bar{f}^t(v_1) \\
 w_2 &= 2v_1 \times \bar{v}_1 + f(\bar{v}_2) - \bar{f}(v_2) \\
 g(x) &= (-2x \cdot \bar{v}_1)v_2 + (2x \cdot v_1)\bar{v}_2 + v_1 \times (\bar{v}_2 \times x) \\
 &\quad - \bar{v}_1 \times (v_2 \times x) + [f, \bar{f}](x), \quad x \in V
 \end{aligned}
 \tag{**}$$

(see [Se1,(23),(24)]).

We have the following

**Lemma 2.6.2** *The map*

$$\begin{aligned}
 \phi : L &\rightarrow L \\
 (v_1, v_2, f) &\mapsto (v_2, v_1, -f^t)
 \end{aligned}$$

*is an involutory automorphism of  $L$ .*

**Proof** This follows from a routine calculation using  $(**)$  and the definition of the transpose map above. Alternatively, we can show that, for  $\delta \in L$ ,  $\phi(\delta) = -\delta^t$ , where  $\delta^t$  is the transpose of  $\delta$  with respect to the scalar product:  $c_i \hat{c}_i = 1$ ,  $c_i \hat{c}_j = 0$ ,  $i \neq j$  (also see 2.7.2(i)).  $\square$

The following can then be taken as a set of root vectors corresponding to a Chevalley basis of  $L$  (see [Se1,below (24)]):

$$\begin{aligned}
 e_{\alpha_1} &= (e_1, 0, 0) & e_{-\alpha_1} &= (0, -e_1, 0) \\
 e_{\alpha_2} &= (0, 0, E_{12}) & e_{-\alpha_2} &= (0, 0, E_{21}) \\
 e_{\alpha_1+\alpha_2} &= (e_2, 0, 0) & e_{-(\alpha_1+\alpha_2)} &= (0, -e_2, 0) \\
 e_{2\alpha_1+\alpha_2} &= (0, e_3, 0) & e_{-(2\alpha_1+\alpha_2)} &= (-e_3, 0, 0) \\
 e_{3\alpha_1+\alpha_2} &= (0, 0, E_{31}) & e_{-(3\alpha_1+\alpha_2)} &= (0, 0, E_{13}) \\
 e_{3\alpha_1+2\alpha_2} &= (0, 0, E_{32}) & e_{-(3\alpha_1+2\alpha_2)} &= (0, 0, E_{23})
 \end{aligned}$$

The elements  $h_1 = (0, 0, E_{11} - E_{33})$ ,  $h_2 = (0, 0, E_{22} - E_{33})$  span the corresponding (2-dimensional) Cartan subalgebra of  $L$ . The simple roots satisfy  $\alpha_1(h_1) = -1$ ,  $\alpha_1(h_2) = 0$ ,  $\alpha_2(h_1) = 1$ , and  $\alpha_2(h_2) = -1$ . For each  $\alpha \in \Phi^+$ , it is readily checked that  $[e_\alpha, e_{-\alpha}] = h_\alpha$ , the coroot corresponding to  $\alpha$ . Now  $\phi(e_\alpha) = -e_{-\alpha}$ , for all  $\alpha \in \Phi$ , where  $\phi$  is the map

defined in 2.6.2. Therefore the set  $\{h_{\alpha_i}, e_{\alpha} : \alpha_i \in \Delta, \alpha \in \Phi\}$  is a Chevalley basis of  $L$  (also see [C1,4.1] and [H1,25.2]).

Given  $\delta \in L$  we have  $\delta(1) = \delta(11) = \delta(1)1 + 1\delta(1) = 2\delta(1)$ , and so  $\delta(1) = 0$ . Moreover, since  $C' = C_0$ , we have  $\delta(C_0) \subseteq C_0$  (which also follows from  $(*)$  in 2.6.1). Therefore  $\delta$  is completely determined by its restriction to  $C_0$ , with  $C_0$  invariant under  $L$  (and commutation induces a faithful representation  $\delta \mapsto \delta|_{C_0}$ ). For convenience we list below the actions of the *positive* root vectors on the basis  $\beta' = \{c_1 - c_2, c_3, c_4, c_5, c_6, c_7, c_8\}$  of  $C_0$ , calculated using  $(*)$  in 2.6.1. In each case the basis elements sent to 0 are omitted.

$$\begin{array}{lll}
e_{\alpha_1} : c_1 - c_2 \mapsto 2c_3 & e_{\alpha_2} : c_3 \mapsto -c_4 & e_{\alpha_1+\alpha_2} : c_1 - c_2 \mapsto 2c_4 \\
c_4 \mapsto c_8 & c_7 \mapsto c_6 & c_3 \mapsto -c_8 \\
c_5 \mapsto -c_7 & & c_5 \mapsto c_6 \\
c_6 \mapsto -(c_1 - c_2) & & c_7 \mapsto -(c_1 - c_2) \\
\\
e_{2\alpha_1+\alpha_2} : c_1 - c_2 \mapsto 2c_8 & e_{3\alpha_1+\alpha_2} : c_5 \mapsto -c_3 & e_{3\alpha_1+2\alpha_2} : c_5 \mapsto -c_4 \\
c_5 \mapsto -(c_1 - c_2) & c_6 \mapsto c_8 & c_7 \mapsto c_8 \\
c_6 \mapsto c_4 & & \\
c_7 \mapsto -c_3 & & 
\end{array}$$

We have the following

**Lemma 2.6.3** *Let*

$$N = \sum_{\text{ht}(\alpha)=1} e_{\alpha} = e_{\alpha_1} + e_{\alpha_2} \in L = \text{Der } \mathcal{C}.$$

*Then  $N^5 = N^{\text{ht}(r_0)} = 2e_{r_0} \in L$ , and  $N^i = 0$ ,  $i \geq 7$ .*

**Proof** By the above we have

$$\begin{array}{ll}
N = e_{\alpha_1} + e_{\alpha_2} : c_1 - c_2 \mapsto 2c_3 & N^2 : c_1 - c_2 \mapsto -2c_4 \\
c_3 \mapsto -c_4 & c_3 \mapsto -c_8 \\
c_4 \mapsto c_8 & c_5 \mapsto -c_6 \\
c_5 \mapsto -c_7 & c_6 \mapsto -2c_3 \\
c_6 \mapsto -(c_1 - c_2) & c_7 \mapsto -(c_1 - c_2) \\
c_7 \mapsto c_6 & 
\end{array}$$

$$\begin{array}{lll}
N^3 : c_1 - c_2 \mapsto -2c_8 & N^4 : c_5 \mapsto 2c_3 & N^5 : c_5 \mapsto -2c_4 \\
c_5 \mapsto c_1 - c_2 & c_6 \mapsto 2c_8 & c_7 \mapsto 2c_8 \\
c_6 \mapsto 2c_4 & c_7 \mapsto 2c_4 & \\
c_7 \mapsto -2c_3 & & 
\end{array}$$

Therefore  $N^5 = 2e_{r_0}$  as required.  $\square$

The case of  $N^5$  above agrees nicely with the corresponding results for the classical types. Moreover, the fact that  $N^5 \in L$  is somewhat of a surprise. It is also easy to see that  $N^2 \notin L$  and  $N^3 \notin L$ , these two cases corresponding to the ‘bad’ primes 2 and 3, respectively.

We now obtain a basis of  $\mathcal{C}_0$  with respect to which the matrices representing the (restrictions to  $\mathcal{C}_0$  of the) simple root vectors of  $L$  are height 1 strictly upper triangular matrices. Define  $\beta_0 = \{c_8, c_4, c_3, c_1 - c_2, c_6, c_7, c_5\}$ , a re-ordering of the basis  $\beta'$  of  $\mathcal{C}_0$ . Let  $\phi : L \rightarrow gl(7, \mathbb{C})$  denote the corresponding (faithful) representation. Using p.84, we obtain

$$\begin{aligned}
\phi(e_{\alpha_1}) &= e_{12} + 2e_{34} - e_{45} - e_{67} \\
\phi(e_{\alpha_2}) &= -e_{23} + e_{56} \\
\phi(e_{\alpha_1+\alpha_2}) &= -e_{13} + 2e_{24} - e_{46} + e_{57} \\
\phi(e_{2\alpha_1+\alpha_2}) &= 2e_{14} + e_{25} - e_{36} - e_{47} \\
\phi(e_{3\alpha_1+\alpha_2}) &= e_{15} - e_{37} \\
\phi(e_{3\alpha_1+2\alpha_2}) &= e_{16} - e_{27}
\end{aligned}$$

Let  $\mathcal{A}(F)$  be a non-associative algebra over  $F$ , where  $F = \mathbb{C}$  or  $K$ , an algebraically closed field of characteristic  $p > 2$ . An element  $\theta \in \text{End } \mathcal{A}(F)$  is called an *automorphism* of  $\mathcal{A}(F)$  if the following conditions are satisfied:

$$\theta \text{ is a bijection and } \theta(xy) = \theta(x)\theta(y), \text{ for all } x, y \in \mathcal{A}(F).$$

Let  $\text{Aut } \mathcal{A}(F)$  denote the collection of all such automorphisms, a group under composition. We have the following

**Lemma 2.6.4** [J1,1.2] *Let  $\mathcal{A} = \mathcal{A}(\mathbb{C})$  be a non-associative algebra over  $\mathbb{C}$ . Suppose  $\delta \in \text{Der } \mathcal{A}$  is nilpotent, and write  $\theta = \exp(\delta)$ . Then  $\theta \in \text{Aut } \mathcal{A}$ .*

Given  $\theta \in \text{Aut } \mathcal{C}(F)$  we have  $\theta(1) = \theta(1)1 = \theta(1)\theta(\theta^{-1}(1)) = \theta(1\theta^{-1}(1)) = \theta(\theta^{-1}(1)) = 1$ . Moreover, since  $\mathcal{C}(F)' = \mathcal{C}(F)_0$ , we have  $\theta(\mathcal{C}(F)_0) \subseteq \mathcal{C}(F)_0$  (equality in fact). Therefore  $\theta$  is completely determined by its restriction to  $\mathcal{C}(F)_0$ , which is invariant under  $\text{Aut } \mathcal{C}(F)$ . We now need to distinguish between the cases  $F = \mathbb{C}$  and  $F = K$ . Write  $\mathcal{C} = \mathcal{C}(\mathbb{C})$ ,  $\mathcal{C}_0 = \mathcal{C}(\mathbb{C})_0$  (as above),  $\bar{\mathcal{C}} = \mathcal{C}(K)$ , and  $\bar{\mathcal{C}}_0 = \mathcal{C}(K)_0$ . We shall also use bars to denote elements of  $\bar{\mathcal{C}}$ . Then  $\beta_0 = \{c_8, c_4, c_3, c_1 - c_2, c_6, c_7, c_5\}$  is a basis of  $\mathcal{C}_0$ , and  $\bar{\beta}_0 = \{\bar{c}_8, \bar{c}_4, \bar{c}_3, \bar{c}_1 - \bar{c}_2, \bar{c}_6, \bar{c}_7, \bar{c}_5\}$  is a basis of  $\bar{\mathcal{C}}_0$ . Finally write  $\phi : \text{Aut } \mathcal{C} \rightarrow GL(7, \mathbb{C})$  and  $\bar{\phi} : \text{Aut } \bar{\mathcal{C}} \rightarrow GL(7, K)$  for the corresponding (faithful) representations.

Let  $X = (X_0, X_1, \dots, X_{t-1})$ , where  $t \geq 1$ , be a set of indeterminates. Suppose  $A(X) \in M(7, \mathbb{Z}_{(p)}[X])$ , with  $\det A(X)$  a unit of  $\mathbb{Z}_{(p)}$ , so that  $A(X)^{-1} \in M(7, \mathbb{Z}_{(p)}[X])$ . Given an element  $\lambda = (\lambda_0, \lambda_1, \dots, \lambda_{t-1}) \in W_t(\mathbb{C})$ , we can substitute  $\lambda$  for  $X$  in  $A(X)$ , to obtain a matrix  $A(\lambda) \in M(7, \mathbb{C})$ . Now let  $\bar{A}(X)$  denote the image of  $A(X)$  under the natural homomorphism  $M(7, \mathbb{Z}_{(p)}[X]) \rightarrow M(7, K[X])$ . Given  $\mu = (\mu_0, \mu_1, \dots, \mu_{t-1}) \in W_t(K)$ , we can substitute  $\mu$  for  $X$  in  $\bar{A}(X)$  to obtain a matrix  $\bar{A}(\mu) \in M(7, K)$ . We now prove the following result, which is essentially a reformulation of [C1,4.4.2] and [T1, Lemma 1]:

**Lemma 2.6.5** *Refer to the above for notation. Suppose  $A(\lambda) \in \phi(\text{Aut } \mathcal{C})$  for all  $\lambda \in W_t(\mathbb{C})$ . Then  $\bar{A}(\mu) \in \bar{\phi}(\text{Aut } \bar{\mathcal{C}})$  for all  $\mu \in W_t(K)$ .*

**Proof** The following notation will be used: Let  $R$  be a commutative ring with identity,  $1 \in R$ , and let  $M \in M(7, R)$ . Define

$$\text{diag}(1, M) = \left( \begin{array}{c|ccc} 1 & 0 & \dots & 0 \\ \hline 0 & & & \\ \vdots & & M & \\ 0 & & & \end{array} \right) \in M(8, R).$$

Let  $\gamma = \{1\} \cup \beta_0 = \{v_i\}$  and  $\bar{\gamma} = \{\bar{1}\} \cup \bar{\beta}_0 = \{\bar{v}_i\}$ ,  $1 \leq i \leq 8$  (where  $1 = c_1 + c_2$  and  $\bar{1} = \bar{c}_1 + \bar{c}_2$ ), then  $\gamma$  and  $\bar{\gamma}$  are (ordered) bases of  $\mathcal{C}$  and  $\bar{\mathcal{C}}$ , respectively. For  $1 \leq i, j \leq 8$ , we have

$$(*) \quad v_i v_j = \sum_{k=1}^8 \varepsilon_{ijk} v_k,$$

for some  $\varepsilon_{ijk} \in \mathbb{Z}_{(p)}$ . In fact it is clear from the multiplication table on p.81, that at most two basis vectors occur in this sum, with coefficients from the set  $\{-1, -1/2, 1/2, 1\}$ . We also have

$$\bar{v}_i \bar{v}_j = \sum_{k=1}^8 \bar{\varepsilon}_{ijk} \bar{v}_k,$$

where  $\bar{\varepsilon}_{ijk}$  is the image of  $\varepsilon_{ijk}$  under the natural homomorphism  $\mathbb{Z}_{(p)} \rightarrow K$ .

Now (by assumption)  $B(X) = \text{diag}(1, A(X)) \in M(8, \mathbb{Z}_{(p)}[X])$ , and  $B^{-1}(X) = B(X)^{-1} = \text{diag}(1, A(X)^{-1}) \in M(8, \mathbb{Z}_{(p)}[X])$ . Therefore

$$(*)_2 \quad \bar{B}(X) \bar{B}^{-1}(X) = \bar{I}_8 = \bar{B}^{-1}(X) \bar{B}(X),$$

bars denoting images under the natural homomorphism  $M(8, \mathbb{Z}_{(p)}[X]) \rightarrow M(8, K[X])$ . Let  $\lambda = (\lambda_0, \lambda_1, \dots, \lambda_{t-1}) \in W_t(\mathbb{C})$ , and write  $f(\lambda)$  for the *automorphism* of  $\mathcal{C}$  represented by  $B(\lambda) = \text{diag}(1, A(\lambda))$  with respect to  $\gamma$  (see the remarks after 2.6.4). Now let  $\mu = (\mu_1, \mu_2, \dots, \mu_{t-1}) \in W_t(K)$ , and write  $\bar{f}(\mu)$  for the *linear transformation* of  $\bar{\mathcal{C}}$  represented by  $\bar{B}(\mu) = \text{diag}(\bar{1}, \bar{A}(\mu))$  with respect to  $\bar{\gamma}$ . By  $(*)_2$  we have

$$\bar{B}(\mu) \bar{B}^{-1}(\mu) = \bar{I}_8 = \bar{B}^{-1}(\mu) \bar{B}(\mu),$$

and so  $\bar{f}(\mu)$  is *bijective*. Now  $f(\lambda)(v_i) = \sum_{j=1}^8 B(\lambda)_{ji} v_j$  and  $\bar{f}(\mu)(\bar{v}_i) = \sum_{j=1}^8 \bar{B}(\mu)_{ji} \bar{v}_j$ . Applying the automorphism  $f(\lambda)$  to both sides of  $(*)_1$  gives

$$\sum_{1 \leq r, s \leq 8} B(\lambda)_{ri} B(\lambda)_{sj} \left( \sum_{l=1}^8 \varepsilon_{rsl} v_l \right) = \sum_{k=1}^8 \varepsilon_{ijk} \left( \sum_{l=1}^8 B(\lambda)_{lk} v_l \right).$$

Equating coefficients of basis elements gives

$$\sum_{1 \leq r, s \leq 8} B(\lambda)_{ri} B(\lambda)_{sj} \varepsilon_{rsl} = \sum_{k=1}^8 \varepsilon_{ijk} B(\lambda)_{lk},$$

for all  $1 \leq i, j, l \leq 8$ . Since this holds for all  $\lambda \in W_t(\mathbb{C})$ , it follows that the polynomial

$$\sum_{1 \leq r, s \leq 8} B(X)_{ri} B(X)_{sj} \varepsilon_{rsl} - \sum_{k=1}^8 \varepsilon_{ijk} B(X)_{lk} \in \mathbb{Z}_{(p)}[X]$$

is identically zero. Therefore the polynomial

$$\sum_{1 \leq r, s \leq 8} \bar{B}(X)_{ri} \bar{B}(X)_{sj} \bar{\varepsilon}_{rsl} - \sum_{k=1}^8 \bar{\varepsilon}_{ijk} \bar{B}(X)_{lk} \in K[X]$$

is also identically zero, and so

$$\sum_{1 \leq r, s \leq 8} \bar{B}(\mu)_{ri} \bar{B}(\mu)_{sj} \bar{e}_{rsl} = \sum_{k=1}^8 \bar{e}_{ijk} \bar{B}(\mu)_{lk}.$$

It follows that  $\bar{f}(\mu) \in \text{Aut } \bar{\mathcal{C}}$  (and so  $\bar{A}(\mu) \in \bar{\phi}(\text{Aut } \bar{\mathcal{C}})$ ), as required.  $\square$

Let  $K$  be an algebraically closed field of characteristic  $p > 2$ . We now introduce the Chevalley group  $G(K)$  corresponding to the complex simple Lie algebra  $L = \text{Der } \mathcal{C}$ . In the notation of 2.1 we have, for  $t \in K$ ,

$$\begin{aligned} x_{\alpha_1}(t) &= \bar{I} + t(\bar{e}_{12} + 2\bar{e}_{34} - \bar{e}_{45} - \bar{e}_{67}) - t^2 \bar{e}_{35} \\ x_{\alpha_2}(t) &= \bar{I} + t(-\bar{e}_{23} + \bar{e}_{56}) \\ (***) \quad x_{\alpha_1 + \alpha_2}(t) &= \bar{I} + t(-\bar{e}_{13} + 2\bar{e}_{24} - \bar{e}_{46} + \bar{e}_{57}) - t^2 \bar{e}_{26} \\ x_{2\alpha_1 + \alpha_2}(t) &= \bar{I} + t(2\bar{e}_{14} + \bar{e}_{25} - \bar{e}_{36} - \bar{e}_{47}) - t^2 \bar{e}_{17} \\ x_{3\alpha_1 + \alpha_2}(t) &= \bar{I} + t(\bar{e}_{15} - \bar{e}_{37}) \\ x_{3\alpha_1 + 2\alpha_2}(t) &= \bar{I} + t(\bar{e}_{16} - \bar{e}_{27}) \end{aligned}$$

(note that  $x_\alpha(t) \in \bar{\phi}(\text{Aut } \bar{\mathcal{C}})$ , for all  $\alpha \in \Phi^+$ , by 2.6.5). It is shown in [Se1,6] that  $G(K) = \bar{\phi}(\text{Aut } \bar{\mathcal{C}})$ ; it is the simple algebraic group of type  $G_2$  defined over  $K$ , both simply-connected and adjoint. Write  $G = G(K)$  for brevity. We have  $U = \langle X_\alpha : \alpha \in \Phi^+ \rangle \subseteq G \cap U(7, K)$ , and so  $U = (G \cap U(7, K))^\circ$ . In fact  $U = G \cap U(7, K)$  (the previous equality does however suffice for our purposes). We can see this (indirectly) as follows: Write  $\hat{U} = G \cap U(7, K) \subseteq B_u$ , for some Borel subgroup  $B$  of  $G$  (see [H2,30.4]). There exists  $x \in G$  with  ${}^x \hat{U} \subseteq U = \hat{U}^\circ$ , and so  $({}^x \hat{U})^\circ \subseteq \hat{U}^\circ$ . This forces  $({}^x \hat{U})^\circ = U$  (for dimension reasons). Therefore  ${}^x \hat{U} = ({}^x \hat{U})^\circ$ , and so  $\hat{U} = \hat{U}^\circ$ , as required.  $\square$

The following result is well-known:

**Lemma 2.6.6** *Let  $u \in U = G \cap U(7, K)$ , then the following hold:*

- (i)  $u(1) = (\mu_1, -\mu_2, 2\mu_1, -\mu_1, \mu_2, -\mu_1)$ , for some  $\mu_1, \mu_2 \in K$ .
- (ii)  $u$  is regular  $\Leftrightarrow \mu_1, \mu_2 \neq 0$ .

**Proof** Argue as in the proof of 2.2.3, using (\*\*\*) above.  $\square$



We now come to the main result of this section. The proof uses notation from 1.7.

**Theorem 2.6.7** *Let  $G(K) = \overline{\phi}(\text{Aut } \overline{\mathcal{C}})$ , where  $K$  is an algebraically closed field of characteristic  $p > 3$ . Suppose  $u \in G(K)_u$  is a regular unipotent element. Then the following hold:*

$$(i) \quad o(u) = p^t = \min\{p^s : s \in \mathbb{N} \text{ and } p^s > \text{ht}(r_0)\}.$$

(ii) *There exists a closed subgroup  $V$  of  $G(K)$ , with  $V \cong W_t(K)$  and  $u \in V$ .*

**Proof** Define  $\text{Stab } \mathcal{C}_0 = \{f \in \text{End } \mathcal{C} : f(\mathcal{C}_0) \subseteq \mathcal{C}_0\}$ , and let  $\phi : \text{Stab } \mathcal{C}_0 \rightarrow M(7, \mathbb{C})$  denote the corresponding (algebra) map, where for  $f \in \text{Stab } \mathcal{C}_0$ ,  $\phi(f)$  is the matrix representing  $f|_{\mathcal{C}_0}$  with respect to  $\beta_0$ . We have  $L = \text{Der } \mathcal{C} \subseteq \text{Stab } \mathcal{C}_0$  and  $G(\mathbb{C}) = \text{Aut } \mathcal{C} \subseteq \text{Stab } \mathcal{C}_0$ . We will now identify  $L$  and  $G(\mathbb{C})$  with their images under  $\phi$ . Let  $N = e_{\alpha_1} + e_{\alpha_2} \in L$ . Then  $0 \neq N$  is nilpotent, with  $p\text{-nilp}(N) = t$ , where

$$t = \begin{cases} 2 & : p = 5 \\ 1 & : p > 5 \end{cases},$$

as can be seen directly, or use 2.6.3. First suppose  $p = 5$ . Define  $X = (X_0, X_1)$  and  $d(X, N) = X_0 N + (X_0^5/5 + X_1)N^5$ . Then we have

$$A(X) = \exp(d(X, N)) = \sum_{i=0}^6 c(X)_i N^i \in M(7, \mathbb{Z}_{(5)}[X])$$

(see 1.7, where  $E(X)$  is used instead of  $A(X)$ ). Moreover  $\det A(X) = 1$ , and so  $A(X)^{-1} \in M(7, \mathbb{Z}_{(5)}[X])$ . (In fact, since 5 is odd, we have  $A(X)^{-1} = A(-X)$ , where  $-X = (-X_0, -X_1)$ .) Let  $x = (x_0, x_1) \in W_2(\mathbb{C})$ . Substituting  $x$  for  $X$  in  $d(X, N)$  gives

$$d(x, N) = x_0 N + (x_0^5/5 + x_1) N^5 \in L,$$

by 2.6.3. It then follows from 2.6.4 that

$$A(x) = \exp(d(x, N)) = \sum_{i=0}^6 c(x)_i N^i \in G(\mathbb{C})$$

(also see 1.7). Now let  $y = (y_0, y_1) \in W_2(K)$ . Write  $\overline{A}(X)$  for the image of  $A(X)$  under the natural homomorphism  $\psi_7 : M(7, \mathbb{Z}_{(5)}[X]) \rightarrow M(7, K[X])$ , as defined in (†) of 2.2. Then

substituting  $y$  for  $X$  in  $\overline{A}(X)$  gives  $\overline{A}(y) \in G(K)$  by 2.6.5; indeed,  $\overline{A}(y) \in U = G(K) \cap U(7, K)$ . We have

$$\overline{A}(X) = \sum_{i=0}^6 \overline{c}(X)_i \overline{N}^i \in M(7, K[X])$$

(where  $\overline{N} = \psi_7(N)$ ). Moreover  $5\text{-nilp}(\overline{N}) = 5\text{-nilp}(N) = 2$  (see 2.6.3). Therefore

$$\overline{A}(y) = \sum_{i=0}^6 \overline{c}(y)_i \overline{N}^i = e_5(\overline{N}, y),$$

the Artin-Hasse exponential of  $\overline{N}$  with respect to  $y$  (see (27) of chapter 1).

Next suppose  $p > 5$ . Define  $X = (X_0)$ ,  $d(X, N) = X_0 N$ , and  $A(X) = \exp(d(X, N))$ . Then  $A(X), A(X)^{-1} \in M(7, \mathbb{Z}_{(p)}[X])$  (here  $A(X)^{-1} = A(-X)$ , where  $-X = (-X_0)$ ). Now proceed as above, working in one variable instead of two. The argument then concludes as in the proof of 2.2.4, using 2.6.3 and 2.6.6.  $\square$

Write  $G = G(K)$  for brevity, and assume  $p = 5$ . Let  $u \in G_u$  be a regular unipotent element. Since  $\text{rk}(G) = 2$ , we have  $V = Z_G(u)^\circ$ , where  $V$  is the group constructed above (see 2.1). Moreover  $Z_G(u)$  is *connected* by 2.1.2(i), since  $Z(G) = 1$ . Therefore  $Z_G(u) \cong W_2(K)$ .

A direct calculation, using Appendix A, shows that

$$e_5(\overline{N}, y) = x_{\alpha_1}(y_0)x_{\alpha_2}(y_0)x_{\alpha_1+\alpha_2}(2y_0^2)x_{2\alpha_1+\alpha_2}(2y_0^3)x_{3\alpha_1+\alpha_2}(y_0^4)x_{3\alpha_1+2\alpha_2}(3y_0^5+2y_1),$$

$$e_p(\overline{N}, y) = x_{\alpha_1}(y_0)x_{\alpha_2}(y_0)x_{\alpha_1+\alpha_2}(-y_0^2/2)x_{2\alpha_1+\alpha_2}(y_0^3/3)x_{3\alpha_1+\alpha_2}(-y_0^4/4)x_{3\alpha_1+2\alpha_2}(y_0^5/10),$$

where  $y = (y_0, y_1) \in W_2(K)$ ,  $p = 5$ , and  $y = (y_0) \in W_1(K)$ ,  $p > 5$ , respectively.

## 2.7 Type $F_4$

We begin this section with a brief account of the complex simple Lie algebra of type  $F_4$ . For more details, consult [Sc,IV] and [Se2]. Let  $F = \mathbb{C}$  or  $K$ , an algebraically closed field of characteristic  $p > 0$ ,  $p \neq 2, 3$ . Let  $\mathcal{C}(F)$  denote the Cayley algebra introduced in 2.6, juxtaposition denoting algebra multiplication, with basis  $\{c_1, c_2, \dots, c_8\}$ . Given

$$x = \begin{pmatrix} \alpha & v \\ w & \beta \end{pmatrix} \in \mathcal{C}(F),$$

define

$$\bar{x} = \begin{pmatrix} \alpha & v \\ w & \beta \end{pmatrix}^- = \begin{pmatrix} \beta & -v \\ -w & \alpha \end{pmatrix}.$$

Then the map  $\bar{\phi} : x \mapsto \bar{x}$  is an involutory *anti-automorphism* of  $\mathcal{C}(F)$  (that is,  $(xy)^- = \bar{y}\bar{x}$  for all  $x, y \in \mathcal{C}(F)$ ). Recall  $\mathcal{C}(F) = \mathcal{C}(F)_0 \oplus F1$ , where  $1 = c_1 + c_2$  (see 2.6). We have  $\bar{1} = 1$  and  $\bar{x} = -x$  for all  $x \in \mathcal{C}(F)_0$ . For  $x, y \in \mathcal{C}(F)$  define

$$(x, y) = \text{tr}(x\bar{y}),$$

then it is easy to see that  $(,)$  is a non-degenerate symmetric bilinear form on  $\mathcal{C}(F)$  of maximal Witt index 4. Note that  $(x, y)1 = x\bar{y} + y\bar{x} = \bar{x}y + \bar{y}x$ , for all  $x, y \in \mathcal{C}(F)_0$ . Let  $\gamma = \{u_1, u_2, u_3, u_4, u_5, u_6, u_7, u_8\} = \{c_6, c_7, c_8, c_1, -c_3, -c_4, -c_5, c_2\}$ , then the matrix representing  $(,)$  with respect to the basis  $\gamma$  of  $\mathcal{C}(F)$  is

$$A = \left( \begin{array}{c|c} 0 & I_4 \\ \hline I_4 & 0 \end{array} \right)$$

(use the multiplication table for  $\mathcal{C}(F)$  given in 2.6). Let  $T \in \text{End } \mathcal{C}(F)$ . We call  $T$  *skew* relative to  $(,)$  if  $(Tx, y) = -(x, Ty)$ , for all  $x, y \in \mathcal{C}(F)$ . The set of all such skew transformations form a Lie algebra of type  $D_4$ , which we also denote by  $D_4$ . We shall also require the following *principle of triality*: Let  $T \in D_4$  then there exists unique  $T^\psi, T^\phi \in D_4$  such that

$$T^\psi(xy) = (Tx)y + x(T^\phi y),$$

for all  $x, y \in \mathcal{C}(F)$ . The maps  $T \mapsto T^\psi$  and  $T \mapsto T^\phi$  are automorphisms of  $D_4$  (see [J3,1,2] and [Sc,III,8,3.31]).

We can now define the *split exceptional Jordan algebra*  $\mathcal{J}(F)$ . As a set  $\mathcal{J}(F)$  consists of all  $3 \times 3$  matrices of the form

$$a = \begin{pmatrix} \alpha_{11} & a_{12} & a_{13} \\ \bar{a}_{12} & \alpha_{22} & a_{23} \\ \bar{a}_{13} & \bar{a}_{23} & \alpha_{33} \end{pmatrix} = \text{diag}\{\alpha_{11}, \alpha_{22}, \alpha_{33}\} + a_{12}(1, 2) + a_{13}(1, 3) + a_{23}(2, 3),$$

where  $\alpha_{ii} \in F$ ,  $a_{ij} \in \mathcal{C}(F)$ ,  $1 \leq i, j \leq 3$ . Addition and scalar multiplication are defined in the usual way for matrices. The algebra multiplication  $\cdot$  in  $\mathcal{J}(F)$  is defined as follows:

$$a \cdot b = a * b + b * a, \quad a, b \in \mathcal{J}(F),$$

where  $a * b$  denotes the usual multiplication of matrices. For this to make sense, we need to identify  $\alpha \in F$  with  $\alpha 1 \in \mathcal{C}(F)$ . This gives  $\mathcal{J}(F)$  the structure of a 27-dimensional commutative algebra, satisfying the *Jordan identity*:  $(x \cdot y) \cdot x^2 = x \cdot (y \cdot x^2)$  for all  $x, y \in \mathcal{J}(F)$ . We fix a basis  $\beta = \{v_0, v_1, v_2, \dots, v_{26}\}$ , where

$$v_0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad v_1 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad v_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

$$v_{2+i} = \begin{pmatrix} 0 & u_i & 0 \\ \bar{u}_i & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad v_{10+i} = \begin{pmatrix} 0 & 0 & u_i \\ 0 & 0 & 0 \\ \bar{u}_i & 0 & 0 \end{pmatrix}, \quad v_{18+i} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & u_i \\ 0 & \bar{u}_i & 0 \end{pmatrix},$$

$1 \leq i \leq 8$ . Note that  $1 = (v_0 + v_1 + v_2)/2 = I_3/2$  is the identity element in  $\mathcal{J}(F)$ . The multiplication table for  $\mathcal{J}(F)$  can be deduced from the following calculations. Note that  $v_i \cdot v_j = v_j \cdot v_i$ . Any basis product omitted is zero, as of course are many of the products below.

$$\begin{array}{lll} v_0 \cdot v_0 & = & 2v_0 \\ v_0 \cdot v_{2+i} & = & v_{2+i} \\ v_0 \cdot v_{10+i} & = & v_{10+i} \\ v_1 \cdot v_1 & = & 2v_1 \\ v_1 \cdot v_{2+i} & = & v_{2+i} \\ v_1 \cdot v_{18+i} & = & v_{18+i} \\ v_2 \cdot v_2 & = & 2v_2 \\ v_2 \cdot v_{10+i} & = & v_{10+i} \\ v_2 \cdot v_{18+i} & = & v_{18+i} \end{array},$$

$$\begin{array}{ll} v_{2+i} \cdot v_{2+j} & = (u_i, u_j)(v_0 + v_1) \\ v_{2+i} \cdot v_{10+j} & = \bar{u}_i u_j e_{23} + (\bar{u}_i u_j)^- e_{32} \\ v_{2+i} \cdot v_{18+j} & = u_i u_j e_{13} + (u_i u_j)^- e_{31} \\ v_{10+i} \cdot v_{10+j} & = (u_i, u_j)(v_0 + v_2) \\ v_{10+i} \cdot v_{18+j} & = u_i \bar{u}_j e_{12} + (u_i \bar{u}_j)^- e_{21} \\ v_{18+i} \cdot v_{18+j} & = (u_i, u_j)(v_1 + v_2) \end{array},$$

where  $1 \leq i, j \leq 8$ . For example  $v_3 \cdot v_{12} = -v_{25}$ .

Given

$$a = \begin{pmatrix} \alpha_{11} & a_{12} & a_{13} \\ \bar{a}_{12} & \alpha_{22} & a_{23} \\ \bar{a}_{13} & \bar{a}_{23} & \alpha_{33} \end{pmatrix} \in \mathcal{J}(F),$$

we shall define (as usual)  $\text{tr}(a) = \alpha_{11} + \alpha_{22} + \alpha_{33} \in F$ . Define  $\mathcal{J}(F)_0 = \{a \in \mathcal{J}(F) : \text{tr}(a) = 0\}$ . Then  $\mathcal{J}(F)_0$  is a vector subspace of  $\mathcal{J}(F)$ , with basis  $\beta' = \{v_0 - v_1, v_1 - v_2, v_3, v_4, \dots, v_{26}\}$ . Moreover  $\mathcal{J}(F)_0 \cap F1 = 0$ , and so  $\mathcal{J}(F) = \mathcal{J}(F)_0 \oplus F1$ . Indeed

$$\begin{pmatrix} \alpha_{11} & a_{12} & a_{13} \\ \bar{a}_{12} & \alpha_{22} & a_{23} \\ \bar{a}_{13} & \bar{a}_{23} & \alpha_{33} \end{pmatrix} = \begin{pmatrix} (2\alpha_{11} - \alpha_{22} - \alpha_{33})/3 & a_{12} & a_{13} \\ \bar{a}_{12} & (2\alpha_{22} - \alpha_{11} - \alpha_{33})/3 & a_{23} \\ \bar{a}_{13} & \bar{a}_{23} & (2\alpha_{33} - \alpha_{11} - \alpha_{22})/3 \end{pmatrix} \\ + \frac{\alpha_{11} + \alpha_{22} + \alpha_{33}}{3} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in \mathcal{J}(F)_0 + F1, \quad 1 = I_3/2.$$

Let  $\mathcal{J}(F)^*$  denote the subspace of  $\mathcal{J}(F)$  spanned by all *associators*  $(a, b, c) = (a \cdot b) \cdot c - a \cdot (b \cdot c)$ ,  $a, b, c \in \mathcal{J}(F)$ . It follows from the Jordan identity that  $\text{tr}((a, b, c)) = 0$  (see [Sc, IV, 3, p110]), and so  $\mathcal{J}(F)^* \subseteq \mathcal{J}(F)_0$ . Now  $(v_0, v_3, v_7) = -(v_0 - v_1)$ ,  $(v_1, v_{19}, v_{23}) = -(v_1 - v_2)$ ,  $(v_0, v_1, v_{2+i}) = -v_{2+i}$ ,  $(v_0, v_2, v_{10+i}) = -v_{10+i}$ ,  $(v_1, v_2, v_{18+i}) = -v_{18+i}$ ,  $1 \leq i \leq 8$ , and so  $\mathcal{J}(F)^* = \mathcal{J}(F)_0$ .

Now consider the case where  $F = \mathbb{C}$  (over which our Lie algebras are defined). Write  $\mathcal{J} = \mathcal{J}(\mathbb{C})$ ,  $\mathcal{J}_0 = \mathcal{J}(\mathbb{C})_0$ ,  $\mathcal{J}^* = \mathcal{J}(\mathbb{C})^*$ , and  $\mathcal{C} = \mathcal{C}(\mathbb{C})$ . Define  $L = \text{Der } \mathcal{J}$ , then  $L$  is the complex simple Lie algebra of type  $F_4$ . If  $\Delta = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$  denotes the set of simple roots

of  $L$ , then the set  $\Phi^+$  of positive roots consists of the elements below:

<u>Height</u>				
1	1000	0100	0010	0001
2	1100	0110	0011	
3	1110	0120	0111	
4	1120	1111	0121	
5	1220	1121	0122	
6	1221	1122		
7	1231	1222		
8	1232			
9	1242			
10	1342			
11	2342			

(where, for example, 1221 denotes the root  $\alpha_1 + 2\alpha_2 + 2\alpha_3 + \alpha_4$ ). The highest root is  $r_0 = 2342$ , of height  $\text{ht}(r_0) = 11$ .

We have the following

**Lemma 2.7.1** [Se2,1] *The map*

$$\begin{aligned} \psi : \mathcal{C} \oplus \mathcal{C} \oplus \mathcal{C} \oplus D_4 &\rightarrow L \\ (a_{12}, a_{13}, a_{23}, T) &\mapsto \delta \end{aligned} ,$$

where

$$\begin{aligned} &\delta (\text{diag}\{\beta_{11}, \beta_{22}, \beta_{33}\} + b_{12}(1, 2) + b_{13}(1, 3) + b_{23}(2, 3)) \\ = &\text{diag}\{-(b_{12}, a_{12}) - (b_{13}, a_{13}), (b_{12}, a_{12}) - (b_{23}, a_{23}), (b_{13}, a_{13}) + (b_{23}, a_{23})\} \\ (*) &+((\beta_{11} - \beta_{22})a_{12} - b_{13}\bar{a}_{23} - a_{13}\bar{b}_{23} + Tb_{12})(1, 2) , \\ &+((\beta_{11} - \beta_{33})a_{13} + b_{12}a_{23} - a_{12}b_{23} + T^\psi b_{13})(1, 3) \\ &+((\beta_{22} - \beta_{33})a_{23} + \bar{b}_{12}a_{13} + \bar{a}_{12}b_{13} + T^\phi b_{23})(2, 3) \end{aligned}$$

is a vector space isomorphism.

From now on we shall write  $\delta = (a_{12}, a_{13}, a_{23}, T)$ , where  $a_{12}, a_{13}, a_{23} \in \mathcal{C}$ ,  $T \in D_4$ , to mean the element  $\delta \in L$  defined by  $(*)$  above. If  $\varepsilon = (b_{12}, b_{13}, b_{23}, U) \in L$ , then  $[\delta, \varepsilon] = (c_{12}, c_{13}, c_{23}, V) \in L$ , where

$$\begin{aligned}
 c_{12} &= -U(a_{12}) + T(b_{12}) + a_{13}\bar{b}_{23} - b_{13}\bar{a}_{23} \\
 c_{13} &= -U^\psi(a_{13}) + T^\psi(b_{13}) + b_{12}a_{23} - a_{12}b_{23} \\
 (**) \quad c_{23} &= -U^\phi(a_{23}) + T^\phi(b_{23}) - \bar{b}_{12}a_{13} + \bar{a}_{12}b_{13} \\
 V(a) &= -2(a, b_{12})a_{12} + 2(a, a_{12})b_{12} + (aa_{23})\bar{b}_{23} - (ab_{23})\bar{a}_{23} \\
 &\quad + b_{13}(\bar{a}_{13}a) - a_{13}(\bar{b}_{13}a) + [T, U](a), \quad a \in \mathcal{C}
 \end{aligned}$$

(see [Se2,1,(14)]).

The following notation will be required: For  $1 \leq i, j \leq 8$ , let  $E_{ij}$  be the linear transformation of  $\mathcal{C}$  sending  $u_j \mapsto u_i$  and  $u_k \mapsto 0$ ,  $k \neq j$ . Now let  $x = \sum_{i=1}^8 \lambda_i u_i$ ,  $y = \sum_{i=1}^8 \mu_i u_i \in \mathcal{C}$ . Define  $x \cdot y = \sum_{i=1}^8 \lambda_i \mu_i$ , the scalar product of  $x$  and  $y$ . If  $T \in \text{End } \mathcal{C}$  then the transpose of  $T$  with respect to  $\cdot$  is the (unique) map  $T^t \in \text{End } \mathcal{C}$  satisfying  $(Tx) \cdot y = x \cdot (T^t y)$ , for all  $x, y \in \mathcal{C}$  (see [L,XIII,5]). In particular,  $E_{ij}^t = E_{ji}$ .

We have the following

**Lemma 2.7.2** *The following hold:*

(i) *The map  $\pi : \mathcal{C} \rightarrow \mathcal{C}$  defined by*

$$\pi \begin{pmatrix} \alpha & v \\ w & \beta \end{pmatrix} = \begin{pmatrix} \beta & -w \\ -v & \alpha \end{pmatrix},$$

*is an involutory automorphism of  $\mathcal{C}$ , satisfying  $\pi(u_i) = u_{i+4}$  and  $\pi(u_{i+4}) = u_i$ , where  $1 \leq i \leq 4$ . Moreover  $\pi \circ \bar{\phi} = \bar{\phi} \circ \pi$ , and  $\pi \circ T = -T^t \circ \pi$ , for all  $T \in D_4$ .*

(ii) *The map  $\theta : L \rightarrow L$  defined by*

$$\theta(a_{12}, a_{13}, a_{23}, T) = (\pi a_{12}, \pi a_{13}, \pi a_{23}, -T^t),$$

*is an involutory automorphism of  $L$ .*

**Proof** Part (i) is readily verified: For the last claim, note that the matrix of  $\pi$  with respect to the basis  $\gamma$  of  $\mathcal{C}$  is just  $A$ , the matrix of the form  $(,)$  with respect to  $\gamma$ , as on p.91. Now let  $r, s \in \mathcal{C}_0$ , and define

$$\begin{array}{ccc} R_r : \mathcal{C} & \rightarrow & \mathcal{C} \\ x & \mapsto & xr \end{array} \quad \text{and} \quad \begin{array}{ccc} L_s : \mathcal{C} & \rightarrow & \mathcal{C} \\ x & \mapsto & sx \end{array}.$$

Then  $R_r$  is right multiplication by  $r$ , and  $L_s$  is left multiplication by  $s$ . Write  $R_0(\mathcal{C}) = \{R_r : r \in \mathcal{C}_0\}$  and  $L_0(\mathcal{C}) = \{L_s : s \in \mathcal{C}_0\}$ . It is shown in [Sc,III,8,(3.76)] that  $\text{Der } \mathcal{C}$ ,  $R_0(\mathcal{C})$ , and  $L_0(\mathcal{C})$  are subspaces of  $D_4$ , and

$$D_4 = \text{Der } \mathcal{C} \oplus R_0(\mathcal{C}) \oplus L_0(\mathcal{C}).$$

First let  $\delta \in \text{Der } \mathcal{C}$ , then  $\delta^t \circ \pi = -\pi \circ \delta$ , and so  $\delta^t \in \text{Der } \mathcal{C}$ , since  $\pi \in \text{Aut } \mathcal{C}$ . Now let  $r, s \in \mathcal{C}_0$ . Then  $R_r^t \circ \pi = -\pi \circ R_r$  implies  $R_r^t = -R_{\pi r}$ . Similarly we get  $L_s^t = -L_{\pi s}$ . The proof of [Sc,III,8,3.31] then makes it clear that

$$(T^t)^\psi = (T^\psi)^t \quad \text{and} \quad (T^t)^\phi = (T^\phi)^t, \quad \text{for all } T \in D_4.$$

(Alternatively, we can argue directly, using [Se2,2].) Now  $[T, U]^t = -[T^t, U^t]$ , for all  $T, U \in \text{End } \mathcal{C}$  (see [L,XIII,5]). Finally note that  $(\pi x, \pi y) = (x, y)$ , for all  $x, y \in \mathcal{C}$ , using the fact that  $(x, y)1 = x\bar{y} + y\bar{x}$ . Part (ii) then follows, using (i) and (\*\*) above.

Alternatively, we can show that, for  $\delta \in L$ ,  $\theta(\delta) = -\delta^i$ , where  $\delta^i$  is the transpose of  $\delta$  with respect to the scalar product  $v_i \hat{\cdot} v_i = 1$ ,  $v_i \hat{\cdot} v_j = 0$ ,  $i \neq j$  (we omit the details).  $\square$



The *positive* root vectors corresponding to a Chevalley basis of  $L$  are given below:

<u>ht1</u> $e_{1000} = (0, 0, 0, E_{23} - E_{76})$	<u>ht2</u> $e_{1100} = (0, 0, 0, -E_{53} + E_{71})$
$e_{0100} = (0, 0, 0, -E_{52} + E_{61})$	$e_{0110} = (u_6, 0, 0, 0)$
$e_{0010} = (u_1, 0, 0, 0)$	$e_{0011} = (0, 0, u_8, 0)$
$e_{0001} = (0, u_5, 0, 0)$	
<u>ht3</u> $e_{1110} = (u_7, 0, 0, 0)$	<u>ht4</u> $e_{1111} = (0, 0, u_2, 0)$
$e_{0111} = (0, 0, u_3, 0)$	$e_{1120} = (0, 0, 0, E_{13} - E_{75})$
$e_{0120} = (0, 0, 0, E_{12} - E_{65})$	$e_{0121} = (0, u_6, 0, 0)$
<u>ht5</u> $e_{1220} = (0, 0, 0, -E_{63} + E_{72})$	<u>ht6</u> $e_{1221} = (0, u_4, 0, 0)$
$e_{1121} = (0, u_7, 0, 0)$	$e_{1122} = (0, 0, 0, -E_{46} + E_{28})$
$e_{0122} = (0, 0, 0, -E_{47} + E_{38})$	
<u>ht7</u> $e_{1231} = (0, 0, u_1, 0)$	<u>ht8</u> $e_{1232} = (u_4, 0, 0, 0)$
$e_{1222} = (0, 0, 0, E_{41} - E_{58})$	
<u>ht9</u> $e_{1242} = (0, 0, 0, -E_{45} + E_{18})$	<u>ht10</u> $e_{1342} = (0, 0, 0, E_{42} - E_{68})$
<u>ht11</u> $e_{2342} = (0, 0, 0, E_{43} - E_{78})$	

(for more details, consult [Se2,1]).

The corresponding Cartan subalgebra is spanned by the elements  $h_i = (0, 0, 0, E_{ii} - E_{i+4, i+4})$ ,  $1 \leq i \leq 4$ . The negative roots are chosen so that  $\theta(e_\alpha) = -e_{-\alpha}$ , for all  $\alpha \in \Phi^+$ , where  $\theta$  is the map defined in 2.7.2(ii). It is readily checked that  $[e_\alpha, e_{-\alpha}] = h_\alpha$ , for all  $\alpha \in \Phi^+$  (use (\*\*) and [Se2,1,(2)]). Therefore the set  $\{h_{\alpha_i}, e_\alpha : \alpha_i \in \Delta, \alpha \in \Phi\}$  is a Chevalley basis of  $L$ . The images of the various  $T \in D_4$  (above) under the triality automorphisms  $\psi$  and  $\phi$  are given in Appendix B.

The following lemma will be used in the proof of the main result (2.7.6) of this section.

**Lemma 2.7.3** *Let  $N = e_{1000} + e_{0100} + e_{0010} + e_{0001} \in L = \text{Der } \mathcal{C}$ . Then the following hold:*

(i)  $[N, e_{2342}] = 0$ .

$$(ii) [N, e_{1231} + e_{1222}] = 0.$$

$$(iii) [N, e_{1220} + e_{1121} + 2e_{0122}] = 0.$$

**Proof** Part (i) is clear. Now  $[N, e_{1231}] = [e_{0001}, e_{1231}] = (u_5 \bar{u}_1, 0, 0, 0) = e_{1232}$ , using (\*\*) and the multiplication table on p.81. Similarly, we have  $[N, e_{1222}] = [e_{0010}, e_{1222}] = -e_{1232}$ . This gives (ii). Now  $[N, e_{1220}] = [e_{0001}, e_{1220}] = e_{1221}$  (note that  $(-E_{63} + E_{72})^\psi = -E_{45} + E_{18}$  from Appendix B). Next we have  $[N, e_{1121}] = [e_{0100}, e_{1121}] + [e_{0001}, e_{1121}] = -e_{1221} - 2e_{1122}$  (since  $(-E_{52} + E_{61})^\psi = -E_{47} + E_{38}$  and  $V(a) = u_7(\bar{u}_5 a) - u_5(\bar{u}_7 a)$ , for all  $a \in \mathcal{C}$ , implies  $V = -2(-E_{46} + E_{28})$ ). Finally  $[N, e_{0122}] = [e_{1000}, e_{0122}] = e_{1122}$ , and (iii) follows.  $\square$

Given  $\delta \in L$  we have  $\delta(1) = 0$ . Now let  $a \in \mathcal{J}$  and consider the following linear transformation of  $\mathcal{J}$ :

$$\begin{array}{ccc} L_a : \mathcal{J} & \rightarrow & \mathcal{J} \\ b & \mapsto & a \cdot b \end{array}.$$

Following [Sc, IV, 3, (4.44)], it is easy to see that  $\text{tr}(L_a) = 18 \text{tr}(a)$  for all  $a \in \mathcal{J}$  (use the basis products on p.92). Since  $\delta \in L$  we have  $L_{\delta a} = [\delta, L_a]$ , and so  $\text{tr}(L_{\delta a}) = \text{tr}([\delta, L_a]) = 0$ . Therefore  $\text{tr}(\delta a) = 0$ , and so  $\delta(\mathcal{J}_0) \subseteq \mathcal{J}_0$ . (Alternatively use the fact that  $\mathcal{J}_0 = \mathcal{J}^*$ , coupled with  $\delta((a, b, c)) = (\delta a, b, c) + (a, \delta b, c) + (a, b, \delta c)$ ,  $a, b, c \in \mathcal{J}$ ; or use (\*) in 2.7.1.) Therefore  $\delta$  is completely determined by its restriction to  $\mathcal{J}_0$ , which is invariant under  $L$ . In Appendix B, we list the actions of the positive root vectors of heights 1, 5, 7, and 11 on the basis  $\beta' = \{v_0 - v_1, v_1 - v_2, v_3, v_4, \dots, v_{26}\}$  of  $\mathcal{J}_0$  (calculated using (\*) in 2.7.1).

We now obtain a basis of  $\mathcal{J}_0$  with respect to which the matrices representing the (restrictions to  $\mathcal{J}_0$  of the) root vectors of  $L$  are strictly upper triangular matrices. Write  $v'_1 = v_0 - v_1$  and  $v'_2 = v_1 - v_2$ , for brevity, and define

$$\begin{array}{cccc} w_1 = v_6 & w_8 = v_{21} & w_{15} = v_7 & w_{22} = v_{24} \\ w_2 = v_{19} & w_9 = v_8 & w_{16} = v_{11} & w_{23} = v_{13} \\ w_3 = v_{14} & w_{10} = v_{26} & w_{17} = v_4 & w_{24} = v_{18} \\ w_4 = v_{17} & w_{11} = v_3 & w_{18} = v_{22} & w_{25} = v_{23} \\ w_5 = v_{16} & w_{12} = v_{15} & w_{19} = v_5 & w_{26} = v_{10} \\ w_6 = v_{20} & w_{13} = v'_1 & w_{20} = v_{25} & \\ w_7 = v_9 & w_{14} = v'_2 & w_{21} = v_{12} & \end{array}.$$

Write  $\beta_0 = \{w_1, w_2, \dots, w_{26}\}$ , a re-ordering of the basis  $\beta'$  of  $\mathcal{J}_0$ . Let  $\phi : L \rightarrow gl(26, \mathbb{C})$  denote the corresponding (faithful) representation. We will identify  $L$  with its image under  $\phi$ . Then we have

$$\begin{aligned}
e_{1000} &= -e_{45} + e_{68} - e_{79} + e_{17,19} - e_{20,22} + e_{21,23} \\
e_{0100} &= -e_{34} + e_{8,10} + e_{9,11} - e_{15,17} - e_{18,20} + e_{23,24} \\
e_{0010} &= -e_{23} - e_{46} + e_{58} + e_{10,12} + 2e_{11,13} - e_{11,14} \\
&\quad - e_{13,15} - e_{16,18} - e_{20,21} + e_{22,23} + e_{24,25} \\
e_{0001} &= -e_{12} - e_{67} + e_{89} + e_{10,11} + e_{12,13} + e_{12,14} \\
&\quad - e_{13,16} - e_{14,16} - e_{15,18} - e_{17,20} + e_{19,22} + e_{25,26}
\end{aligned}$$

We have the following

**Lemma 2.7.4** *Let  $N = e_{1000} + e_{0100} + e_{0010} + e_{0001} \in L = \text{Der } \mathcal{J}$ . Then the following hold:*

- (i)  $N^5 = -2(e_{1220} + e_{1121} + 2e_{0122}) + 5R_5$ ,
- (ii)  $N^7 = 5(e_{1231} + e_{1222}) + 7R_7$ ,
- (iii)  $N^{11} = e_{2342} + 11R_{11}$ ,
- (iv)  $N^{13} = 13R_{13}$ ,

where  $0 \neq R_p \in M(26, \mathbb{Z})$ , with each non-zero entry an element of  $\mathbb{Z} - p\mathbb{Z}$ ,  $p = 5, 7, 11, 13$ . Moreover  $R_5^3 = R_7^3 = 0$  and  $R_{11}^2 = R_{13}^2 = 0$ . Finally we have  $N^{17} = 0$ , with  $N^{16} \neq 0$ .

**Proof** Use the descriptions of the appropriate root vectors given in Appendix B, which also gives the maps  $R_5, R_7, R_{11}$ , and  $R_{13}$ .  $\square$

We have not included the cases  $N^2$  and  $N^3$ , as these correspond to the bad primes 2 and 3, respectively. This result, although not as nice as 2.6.3, is still a good analogue of the classical results, especially when viewed ‘modulo  $p$ ’, under which  $\delta^p \in \text{Der } \mathcal{J}(K)$  for all  $\delta \in \text{Der } \mathcal{J}(K)$ .

We now turn our attention to automorphisms. Let  $F = \mathbb{C}$  or  $K$ , an algebraically closed field of characteristic  $p > 3$ . Write  $\text{Aut } \mathcal{J}(F)$  for the automorphism group of  $\mathcal{J}(F)$ . Given

$\theta \in \text{Aut } \mathcal{J}(F)$  we have  $\theta(1) = 1$ . Now  $\theta(a, b, c) = (\theta a, \theta b, \theta c)$ , where  $a, b, c \in \mathcal{J}(F)$ , and since  $\mathcal{J}(F)^* = \mathcal{J}(F)_0$ , we obtain  $\theta(\mathcal{J}(F)_0) \subseteq \mathcal{J}(F)_0$  (equality in fact). Therefore  $\theta$  is completely determined by its restriction to  $\mathcal{J}(F)_0$ , which is invariant under  $\text{Aut } \mathcal{J}(F)$ . We shall need to distinguish between the cases  $F = \mathbb{C}$  and  $F = K$ . Write  $\mathcal{J} = \mathcal{J}(\mathbb{C})$ ,  $\mathcal{J}_0 = \mathcal{J}(\mathbb{C})_0$  (as above),  $\overline{\mathcal{J}} = \mathcal{J}(K)$ , and  $\overline{\mathcal{J}}_0 = \mathcal{J}(K)_0$ . We shall also use bars to denote elements of  $\overline{\mathcal{J}}$ . Then  $\beta_0 = \{w_1, w_2, \dots, w_{26}\}$  is a basis of  $\mathcal{J}_0$ , and  $\overline{\beta}_0 = \{\overline{w}_1, \overline{w}_2, \dots, \overline{w}_{26}\}$  is a basis of  $\overline{\mathcal{J}}_0$ . Write  $\phi : \text{Aut } \mathcal{J} \rightarrow GL(26, \mathbb{C})$  and  $\overline{\phi} : \text{Aut } \overline{\mathcal{J}} \rightarrow GL(26, K)$  for the corresponding (faithful) representations. We will identify  $\text{Aut } \mathcal{J}$  and  $\text{Aut } \overline{\mathcal{J}}$  with their images under  $\phi$  and  $\overline{\phi}$ , respectively.

Next we introduce the Chevalley group  $G(K)$  corresponding to the complex simple Lie algebra  $L = \text{Der } \mathcal{J}$ . In the notation of 2.1 we have, for  $t \in K$ ,

$$\begin{aligned}
 x_{1000}(t) &= \overline{I} + t(-\overline{e}_{45} + \overline{e}_{68} - \overline{e}_{79} + \overline{e}_{17,19} - \overline{e}_{20,22} + \overline{e}_{21,23}) \\
 x_{0100}(t) &= \overline{I} + t(-\overline{e}_{34} + \overline{e}_{8,10} + \overline{e}_{9,11} - \overline{e}_{15,17} - \overline{e}_{18,20} + \overline{e}_{23,24}) \\
 (* *) \quad x_{0010}(t) &= \overline{I} + t(-\overline{e}_{23} - \overline{e}_{46} + \overline{e}_{58} + \overline{e}_{10,12} + 2\overline{e}_{11,13} - \overline{e}_{11,14} \\
 &\quad - \overline{e}_{13,15} - \overline{e}_{16,18} - \overline{e}_{20,21} + \overline{e}_{22,23} + \overline{e}_{24,25}) - t^2(\overline{e}_{11,15}) \\
 x_{0001}(t) &= \overline{I} + t(-\overline{e}_{12} - \overline{e}_{67} + \overline{e}_{89} + \overline{e}_{10,11} + \overline{e}_{12,13} + \overline{e}_{12,14} - \overline{e}_{13,16} \\
 &\quad - \overline{e}_{14,16} - \overline{e}_{15,18} - \overline{e}_{17,20} + \overline{e}_{19,22} + \overline{e}_{25,26}) - t^2(\overline{e}_{12,16})
 \end{aligned}$$

It is shown in [Se2,4] that  $G(K) = \text{Aut } \overline{\mathcal{J}}$ ; it is the simple algebraic group of type  $F_4$  defined over  $K$ , both simply-connected and adjoint. Write  $G = G(K)$  for brevity. We have  $U = \langle X_\alpha : \alpha \in \Phi^+ \rangle = G \cap U(26, K)$  (see 2.6).

The following result is well-known:

**Lemma 2.7.5** *Let  $u \in U = G \cap U(26, K)$ , then the following hold:*

(i)  $u(1)$  is of the form

$$u(1) = (-\mu_4, -\mu_3, -\mu_2, -\mu_1, \underbrace{*, \dots, *}_{21 \text{ terms}}),$$

where  $\mu_i \in K$ ,  $1 \leq i \leq 4$  (the various  $*$  do not concern us).

(ii)  $u$  is regular  $\Leftrightarrow \mu_i \neq 0$ ,  $1 \leq i \leq 4$ .

**Proof** Argue as in the proof of 2.2.3, using  $(***)$  above. □

We now come to the main result of this section. The proof uses notation from 1.7.

**Theorem 2.7.6** *Let  $G(K) = \text{Aut } \overline{\mathcal{J}}$ , where  $K$  is an algebraically closed field of characteristic  $p > 3$ . Suppose  $u \in G(K)_u$  is a regular unipotent element. Then the following hold:*

(i)  $\text{o}(u) = p^t = \min\{p^s : s \in \mathbb{N} \text{ and } p^s > \text{ht}(r_0)\}$ .

(ii) *There exists a closed subgroup  $V$  of  $G(K)$ , with  $V \cong W_t(K)$  and  $u \in V$ .*

**Proof** Let  $N = e_{1000} + e_{0100} + e_{0010} + e_{0001} \in L = \text{Der } \mathcal{J}$ . Write  $t = p\text{-nilp}(N)$  and  $\bar{t} = p\text{-nilp}(\overline{N})$ . Then, by 2.7.4 and Appendix B, we have

$$\begin{cases} t = \bar{t} = 2 & : & p = 5, 7, 11 \\ t = 2, \bar{t} = 1 & : & p = 13 \\ t = \bar{t} = 1 & : & p \geq 17 \end{cases}.$$

First suppose  $p = 5, 7$ , or  $11$ . Define  $X = (X_0, X_1)$ ,  $d(X, N) = X_0N + (X_0^p/p + X_1)N^p$ , and  $E(X) = \exp(d(X, N))$ . Now  $N^p = H_p + pR_p$ , where

$$H_p = \begin{cases} -2(e_{1220} + e_{1121} + 2e_{0122}) & : & p = 5 \\ 5(e_{1231} + e_{1222}) & : & p = 7 \\ e_{2342} & : & p = 11 \end{cases},$$

and  $0 \neq R_p \in M(26, \mathbb{Z})$ , with  $R_p^3 = 0$  (see 2.7.4). Moreover  $[N, H_p] = 0$  by 2.7.3, and so  $[N, R_p] = [H_p, R_p] = 0$ , since  $[N, N^p] = 0$ . Therefore

$$d(X, N) = (X_0N + (X_0^p/p + X_1)H_p) + (X_0^p + pX_1)R_p \in M(26, \mathbb{Q}[X]).$$

Write  $a(X) = X_0N + (X_0^p/p + X_1)H_p$ ,  $b(X) = (X_0^p + pX_1)R_p$ , and  $A(X) = \exp(a(X))$ , for brevity. Note that  $[a(X), b(X)] = 0$ . Then

$$\begin{aligned} E(X) &= \exp(a(X) + b(X)) = A(X) \exp(b(X)) \\ \Rightarrow A(X) &= E(X) \exp(-b(X)) \in M(26, \mathbb{Z}_{(p)}[X]), \end{aligned}$$

using 1.7 and the fact that  $R_p^3 = 0$ ; also see [B1, IV, 4.10.13]. Moreover  $\det A(X) = 1$ , and so  $A(X)^{-1} \in M(26, \mathbb{Z}_{(p)}[X])$  exists. Now let  $x = (x_0, x_1) \in W_2(\mathbb{C})$ . Substituting  $x$  for  $X$  in

$a(X)$  gives  $a(x) = x_0N + (x_0^p/p + x_1)H_p \in L$ . It then follows from 2.6.4 that

$$A(x) = \exp(a(x)) \in G(\mathbb{C}) = \text{Aut } \mathcal{J}.$$

Next we transfer to  $K$ . Let  $y = (y_0, y_1) \in W_2(K)$ . We have

$$(*)_1 \quad \bar{A}(X) = \bar{E}(X) \left( \bar{I} - X_0^p \bar{R}_p + X_0^{2p} \bar{R}_p^2/2 \right).$$

By 2.7.4 we have  $\bar{R}_p \neq \bar{0}$  and  $R_p^3 = 0$ , and so  $p\text{-nilp}(\bar{R}_p) = 1$  (also see Appendix B). Substituting  $y$  for  $X$  in  $\bar{A}(X)$  gives

$$\bar{A}(y) = e_p(\bar{N}, y) e_p(\bar{R}_p, -y_0^p).$$

Moreover we have  $\bar{A}(y) \in G(K) = \text{Aut } \bar{\mathcal{J}}$  (argue as in the proof of 2.6.5, using the multiplication ‘table’ on p.92). Now define

$$W = \{\hat{y} = (y; -y_0^p) : y = (y_0, y_1) \in W_2(K)\} \subseteq W_2(K) \times W_1(K).$$

It is easy to see that  $W \cong W_2(K)$  (as algebraic groups), under the map  $W_2(K) \rightarrow W$  sending  $y \mapsto \hat{y}$ . By 1.6.4 we have the following two maps

$$(*)_2 \quad \begin{array}{ccc} W_2(K) & \rightarrow & SL(26, K) \\ y = (y_0, y_1) & \mapsto & e_p(\bar{N}, y) \end{array} \quad \text{and} \quad \begin{array}{ccc} W_1(K) & \rightarrow & SL(26, K) \\ y_0 & \mapsto & e_p(\bar{R}_p, y_0) \end{array},$$

which are morphisms of algebraic groups (actually isomorphisms onto their images). Consider the map

$$\begin{array}{ccc} \phi : W & \rightarrow & SL(26, K) \\ \hat{y} & \mapsto & \bar{A}(y) \end{array}.$$

Define  $V = \text{Im } \phi \subseteq G(K)$ . Then  $\phi$  is a morphism of varieties, as can be seen by viewing  $\phi$  as the canonical composition  $W \rightarrow SL(26, K) \times SL(26, K) \rightarrow SL(26, K)$ . Now  $[N, R_p] = 0$  gives  $[\bar{N}, \bar{R}_p] = \bar{0}$ , and it follows from  $(*)_2$  that  $\phi$  is a homomorphism of groups. We next show that  $\phi$  is injective: Let  $\hat{y} \in \ker \phi$ , so that  $\bar{A}(y) = e_p(\bar{N}, y) e_p(\bar{R}_p, -y_0^p) = \bar{I}$ , then

$$y_0 \bar{N} + \sum_{i=2}^{16} \bar{c}(y)_i \bar{N}^i = y_0^p \bar{R}_p + y_0^{2p} \bar{R}_p^2/2.$$

From Appendix B we have  $\text{ht}(R_p) \geq 6$ , and so comparing  $(1, 2)$ -th entries gives  $y_0 = 0$ . Therefore  $e_p(\bar{N}, y) = \bar{I}$ , and so  $y = 0$  by 1.6.4, as required. Next consider the inverse map

$$\begin{array}{ccc} \phi^{-1} : V & \rightarrow & W \\ \bar{A}(y) & \mapsto & \hat{y} \end{array}.$$

The  $(1, 2)$ -th entry of  $\overline{A}(X)$  is  $-X_0$ , and so each coordinate of  $\overline{E}(X)$  is a polynomial in the coordinates of  $\overline{A}(X)$ , by  $(*)_1$ . It then follows from 1.6.3, that  $\phi^{-1}$  is a morphism of varieties. Therefore  $\phi : W \rightarrow V$  is an isomorphism of algebraic groups. Now by 2.7.5,  $V$  contains a regular unipotent element  $v$  (take  $y_0 \neq 0$ ), where  $\text{o}(v) = p^2$  (see 1.2.3(c)), giving the result in this case.

Next consider the case  $p = 13$ . Define  $X = (X_0, X_1)$ ,  $d(X, N) = X_0N + (X_0^{13}/13 + X_1)N^{13}$ , and  $E(X) = \exp(d(X, N))$ . By 2.7.4, we have  $N^{13} = 13R_{13}$ , where  $0 \neq R_{13} \in M(26, \mathbb{Z})$ , with  $R_{13}^2 = 0$ . Write  $A(X_0) = \exp(X_0N)$ , then

$$\begin{aligned} E(X) &= \exp((X_0N) + (X_0^{13} + 13X_1)R_{13}) \\ &= A(X_0) \exp((X_0^{13} + 13X_1)R_{13}) \\ \Rightarrow A(X_0) &= E(X) \exp(-(X_0^{13} + 13X_1)R_{13}) . \end{aligned}$$

It is clear that  $A(X_0), A(X_0)^{-1} \in M(26, \mathbb{Z}_{(13)}[X_0])$ . Let  $x_0 \in W_1(\mathbb{C})$ , then  $x_0N \in L$ , and so  $A(x_0) = \exp(x_0N) \in G(\mathbb{C})$  by 2.6.4. Now let  $y_0 \in W_1(K)$ . We have

$$\overline{A}(X_0) = \overline{E}(X)(\overline{I} - X_0^{13}\overline{R}_{13}) \in M(26, K[X_0]) .$$

By 2.7.4 we have  $\overline{R}_{13} \neq \overline{0}$  and  $R_{13}^2 = 0$ , and so  $13\text{-nilp}(\overline{R}_{13}) = 1$ . Substituting  $y_0$  for  $X_0$  gives

$$\overline{A}(y_0) = e_{13}(\overline{N}, y_0) e_{13}(\overline{R}_{13}, -y_0^{13}) \in G(K)$$

(as above). Finally define  $W = \{\hat{y} = (y_0; -y_0^{13}) : y_0 \in W_1(K)\} \subseteq W_1(K) \times W_1(K)$ , then  $W \cong W_1(K)$ . The argument now proceeds as above.

For the case  $p \geq 17$ , argue as in the proof of 2.6.7. □

## 2.8 Type $E_n$ , $n = 6, 7, 8$

Under the natural embedding  $F_4 \subseteq E_6$ , the regular unipotent elements of the  $F_4$  are also regular in  $E_6$ . It follows that we do not have to consider type  $E_6$  (also see the proof of 2.9.1 to follow). For reasons of space and time, we have been unable to include the case  $E_8$ , but see the remarks after 3.3.3 to follow. This leaves type  $E_7$ , which we discuss below.

Let  $L(\mathbb{C})$  be the complex simple Lie algebra of type  $E_7$ . If  $\Delta = \{\alpha_1, \dots, \alpha_7\}$  denotes the set of simple roots of  $L(\mathbb{C})$ , then the set  $\Phi^+$  of positive roots consists of the following 63 elements:

1	1000000	22	0111100	43	1122110
2	0100000	23	0101110	44	0112211
3	0010000	24	0011110	45	1112210
4	0001000	25	0001111	46	1122111
5	0000100	26	1111100	47	1112211
6	0000010	27	1011110	48	1122210
7	0000001	28	0111110	49	0112221
8	1010000	29	0011111	50	1123210
9	0101000	30	0101111	51	1112221
10	0011000	31	0112100	52	1122211
11	0001100	32	1111110	53	1122221
12	0000110	33	1011111	54	1123211
13	0000011	34	0111111	55	1223210
14	1011000	35	1112100	56	1123221
15	0111000	36	0112110	57	1223211
16	0101100	37	1111111	58	1223221
17	0011100	38	1112110	59	1123321
18	0001110	39	0112111	60	1223321
19	0000111	40	1122100	61	1224321
20	1111000	41	0112210	62	1234321
21	1011100	42	1112111	63	2234321

(where, for example, 1011000 denotes the root  $\alpha_1 + \alpha_3 + \alpha_4$ ). The highest root is  $r_0 = 2234321$ , of height  $\text{ht}(r_0) = 17$ .

Let  $\text{ad} : L(\mathbb{C}) \rightarrow \text{Der } L(\mathbb{C})$  denote the *adjoint* representation of  $L(\mathbb{C})$ , and suppose  $\beta = \{h_{\alpha_i}, e_{\alpha} : \alpha_i \in \Delta, \alpha \in \Phi\}$  is a Chevalley basis of  $L(\mathbb{C})$ . Then we have a vector



space isomorphism  $\phi : \text{End } L(\mathbb{C}) \rightarrow M(133, \mathbb{C})$ , where for  $f \in \text{End } L(\mathbb{C})$ ,  $\phi(f)$  is the matrix representing  $f$  with respect to  $\beta$ . We will identify  $\text{Der } L(\mathbb{C}) = \text{ad } L(\mathbb{C})$  with its image under  $\phi$ . In Appendix C we provide enough information to determine the matrices  $\text{ad} e_\alpha$ , for all  $\alpha \in \Phi$ .

Let  $\alpha \in \Phi^+$  be the  $i$ -th root as labelled above, where  $1 \leq i \leq 63$ . We will write  $e_{(i)}$  for  $e_\alpha$ . Define

$$\begin{aligned} e_r &= \sum_{i=1}^7 e_{(i)} , \\ e_s &= e_{(1)} + e_{(3)} + e_{(10)} + e_{(9)} + e_{(5)} + e_{(6)} + e_{(7)} . \end{aligned}$$

These two elements correspond, respectively, to the regular and subregular unipotent classes in the associated Chevalley group. The reason for including the subregular class in this case (and not the previous cases) is given in 3.2 to follow.

The following two results concerning  $e_r$  and  $e_s$  will be used in the proof of the main result (2.8.5) of this section. Let  $K$  be a field of characteristic  $p > 0$ . As usual, bars denote images under the map defined in (†) of 2.2.

**Lemma 2.8.1** *Let  $N_r = \text{ad} e_r \in \text{Der } L(\mathbb{C})$ . Suppose  $p \geq 5$  is a prime in  $\mathbb{N}$ . Then the following hold:*

(i)  $N_r^p = H_p + pR_p$ , where

$$H_p = \begin{cases} -2\text{ad}(e_{(26)} + 2e_{(27)} - e_{(28)} + 2e_{(29)} - 3e_{(30)} - e_{(31)}) & : p = 5 \\ -2\text{ad}(2e_{(37)} + e_{(38)} - e_{(39)} + e_{(40)} - e_{(41)}) & : p = 7 \\ 56\text{ad}(-e_{(53)} + e_{(54)} + e_{(55)}) & : p = 11 \\ -176\text{ad}(e_{(58)} - e_{(59)}) & : p = 13 \\ -2574\text{ad} e_{(63)} & : p = 17 \\ 0 & : p > 17 \end{cases} .$$

In particular  $H_p \in \text{Der } L(\mathbb{C})$ . Moreover  $H_p, R_p \in M(133, \mathbb{Z})$ . We have  $[N_r, H_p] = 0$ , and so  $[N_r, R_p] = [H_p, R_p] = 0$ . Also  $N_r^{34} \neq 0$  and  $N_r^{35} = 0$ .

(ii) Define  $t = p\text{-nilp}(N_r)$  and  $\bar{t} = p\text{-nilp}(\bar{N}_r)$ . Then we have

$$\begin{cases} t = 3, \bar{t} = 2 & : p = 5 \\ t = \bar{t} = 2 & : p = 7, 11, 13, 17 \\ t = 2, \bar{t} = 1 & : p = 19, 23, 29, 31 \\ t = \bar{t} = 1 & : p > 31 \end{cases}.$$

Moreover  $p\text{-nilp}(R_p) = p\text{-nilp}(\bar{R}_p) = s$ , where

$$s = \begin{cases} 2 & : p = 5 \\ 1 & : p = 7, 11, 13, 17, 19, 23, 29, 31 \end{cases}.$$

If  $p > 31$  then  $R_p = 0$ .

(iii) Let  $p = 5$ . Then  $N_r^{25} = 5S_5$  and  $R_5^5 = S_5 + 5T_5$ , where  $S_5, T_5 \in M(133, \mathbb{Z})$ . We have  $[R_5, S_5] = 0$ , and so  $[R_5, T_5] = [S_5, T_5] = 0$ . Moreover

$$5\text{-nilp}(S_5) = 5\text{-nilp}(\bar{S}_5) = 1$$

$$5\text{-nilp}(T_5) = 5\text{-nilp}(\bar{T}_5) = 1$$

**Proof** This follows from a computer calculation, using Appendix C. □

Next we have

**Lemma 2.8.2** Let  $N_s = \text{ade}_s \in \text{Der } L(\mathbb{C})$ . Suppose  $p \geq 5$  is a prime in  $\mathbb{N}$ . Then the following hold:

(i)  $N_s^p = H'_p + pR'_p$ , where

$$H'_p = \begin{cases} \text{ad}(e_{(32)} - 4e_{(33)} + e_{(34)} + 2e_{(38)} - 2e_{(39)} + 3e_{(40)} - 2e_{(41)}) & : p = 5 \\ -9\text{ad}(e_{(46)} - e_{(47)} + e_{(49)} + e_{(50)}) & : p = 7 \\ 12\text{ad}(e_{(60)} - e_{(61)}) & : p = 11 \\ -462\text{ad}e_{(63)} & : p = 13 \\ 0 & : p > 13 \end{cases}.$$

In particular  $H'_p \in \text{Der } L(\mathbb{C})$ . Moreover  $H'_p, R'_p \in M(133, \mathbb{Z})$ . We have  $[N_s, H'_p] = 0$ , and so  $[N_s, R'_p] = [H'_p, R'_p] = 0$ . Also  $N_s^{26} \neq 0$  and  $N_s^{27} = 0$ .

(ii) Define  $t = p\text{-nilp}(N_s)$  and  $\bar{t} = p\text{-nilp}(\bar{N}_s)$ . Then we have

$$\begin{cases} t = 3, \bar{t} = 2 & : p = 5 \\ t = \bar{t} = 2 & : p = 7, 11, 13 \\ t = 2, \bar{t} = 1 & : p = 17, 19, 23 \\ t = \bar{t} = 1 & : p > 23 \end{cases}.$$

Moreover  $p\text{-nilp}(R'_p) = p\text{-nilp}(\bar{R}'_p) = s$ , where

$$s = \begin{cases} 2 & : p = 5 \\ 1 & : p = 7, 11, 13, 17, 19, 23 \end{cases}.$$

If  $p > 23$  then  $R'_p = 0$ .

(iii) Let  $p = 5$ . Then  $N_s^{25} = 5S'_5$  and  $(R'_5)^5 = S'_5 + 5T'_5$ , where  $S'_5, T'_5 \in M(133, \mathbb{Z})$ . We have

$[R'_5, S'_5] = 0$ , and so  $[R'_5, T'_5] = [S'_5, T'_5] = 0$ . Moreover

$$\begin{aligned} 5\text{-nilp}(S'_5) &= 5\text{-nilp}(\bar{S}'_5) = 1 \\ 5\text{-nilp}(T'_5) &= 5\text{-nilp}(\bar{T}'_5) = 1 \end{aligned}.$$

**Proof** As in 2.8.1. □

We have not included the cases  $N^2$  and  $N^3$  ( $N = N_r$  and  $N_s$ ), as these correspond to the bad primes 2 and 3, respectively. As in type  $F_4$  (see 2.7.4), the results above are a good analogue of the classical results.

Let  $K$  be an algebraically closed field of characteristic  $p > 0$ . We now introduce the Chevalley group  $G(K)$  corresponding to  $L(\mathbb{C})$ . Define  $L(K) = \mathbb{Z}\beta \otimes_{\mathbb{Z}} K$ , where  $\mathbb{Z}\beta$  is the  $\mathbb{Z}$ -span of the Chevalley basis  $\beta$  of  $L(\mathbb{C})$ . Then  $L(K)$  is a Lie algebra over  $K$ , with basis  $\bar{\beta} = \{\bar{v} = v \otimes 1 : v \in \beta\}$ . Let  $\bar{\phi} : \text{End } L(K) \rightarrow M(133, K)$  denote the corresponding isomorphism relative to  $\bar{\beta}$ . Identify  $\text{Aut } L(K) \subseteq \text{End } L(K)$  with its image under  $\bar{\phi}$ . We then have  $G(K) = \text{Aut } L(K)$ ; it is the adjoint simple algebraic group of type  $E_7$  defined over  $K$ , as can be seen from [T1, Lemma 1(2)], for example.

Write  $G = G(K)$  for brevity. Then, in the notation of 2.1,  $U = \langle X_\alpha : \alpha \in \Phi^+ \rangle = G \cap U(133, K)$ ; see 2.6. Suppose  $\alpha \in \Phi^+$  is the  $i$ -th root, where  $1 \leq i \leq 63$  (see p.104). Write  $x_i(t)$  for  $x_\alpha(t)$ , where  $t \in K$ . Then

$$(*) \quad x_i(t) = \bar{I} + t(\text{ad } e_{(i)})^- - t^2 \bar{e}_{64-i, 70+i}.$$

Note that  $\text{ht}(\bar{e}_{64-i,70+i}) = 6 + 2i \geq 8$ .

The following two results are well-known. They are the analogues of 2.2.3, and have been formulated to suit our needs. In both cases we assume  $p > 3$ .

**Lemma 2.8.3** *Suppose  $u = \bar{I} + y_0 \bar{N}_r + y_0^2 \bar{N}_r^2/2 + \bar{M} \in U = G \cap U(133, K)$ , where  $y_0 \in K$  and  $\text{ht}(\bar{M}) \geq 3$ . Then  $u$  is regular if and only if  $y_0 \neq 0$ .*

**Proof** Argue as in the proof of 2.2.3, using (\*) above and Appendix C. □

Define  $u_s = x_1(1)x_3(1)x_{10}(1)x_9(1)x_5(1)x_6(1)x_7(1) \in U$ . Then  $u_s$  is a representative of the class of subregular unipotent elements of  $G$  (see [T2,2.1]). We now have

**Lemma 2.8.4** [T2,1.3] *Suppose  $u = \bar{I} + \bar{N}_s + \bar{N}_s^2/2 + \bar{M} \in U = G \cap U(133, K)$ , where  $\text{ht}(\bar{M}) \geq 4$ . Then  $u$  is conjugate to  $u_s$  in  $G$ .*

**Proof** This follows from [T2,1.3] using 2.1, (\*) above, and Appendix C. Also note that  $\text{ht}(N_s^3) = 4$ . □

We now come to the main result of this section. The proof uses notation from 1.7.

**Theorem 2.8.5** *Let  $G(K) = \text{Aut } L(K)$ , where  $K$  is an algebraically closed field of characteristic  $p > 3$ . Then the following hold:*

(i) *Let  $u \in G(K)$  be a regular unipotent element. Then*

(a)  $\text{o}(u) = p^t = \min\{p^{t'} : t' \in \mathbb{N} \text{ and } p^{t'} > \text{ht}(r_0)\}$ .

(b) *There exists a closed subgroup  $V_r$  of  $G(K)$ , with  $V_r \cong W_t(K)$  and  $u \in V_r$ .*

(ii) *Let  $v \in G(K)$  be a subregular unipotent element. Then*

(a)  $\text{o}(v) = p^s = \min\{p^{s'} : s' \in \mathbb{N} \text{ and } p^{s'} > \text{ht}(r_0) - 4\}$ .

(b) *There exists a closed subgroup  $V_s$  of  $G(K)$ , with  $V_s \cong W_s(K)$  and  $v \in V_s$ .*

**Proof** We shall only prove part (i), with (ii) following in a similar way (using 2.8.2 and 2.8.4). First suppose  $p = 5$ . Define  $X = (X_0, X_1, X_2)$ ,  $d(X, N_r) = X_0 N_r + (X_0^5/5 + X_1) N_r^5 + (X_0^{25}/25 + X_1^5/5 + X_2) N_r^{25}$ , and  $E(X) = \exp(d(X, N_r))$ . By 2.8.1 we have

$$\begin{aligned} d(X, N_r) &= (X_0 N_r + (X_0^5/5 + X_1) H_5) + (X_0^5 R_5 + (X_0^{25}/5 + X_1^5) R_5^5) \\ &\quad - X_0^{25} T_5 + 5(X_1 R_5 + X_2 R_5^5) - 5(X_1^5 + 5X_2) T_5 \end{aligned}$$

Write  $a(X_0, X_1) = X_0 N_r + (X_0^5/5 + X_1) H_5$ ,  $b(X_0, X_1) = -X_0^5 R_5 - (X_0^{25}/5 + X_1^5) R_5^5$ , and  $c(X_0) = X_0^{25} T_5$ . Also write  $A(X_0, X_1) = \exp(a(X_0, X_1))$ ,  $B(X_0, X_1) = \exp(b(X_0, X_1))$ , and  $C(X_0) = \exp(c(X_0))$ . Then

$$A(X_0, X_1) = E(X) B(X_0, X_1) C(X_0) \exp(-5(X_1 R_5 + X_2 R_5^5)) \exp(5(X_1^5 + 5X_2) T_5),$$

since  $N_r$ ,  $H_5$ ,  $R_5$ , and  $T_5$  are mutually commuting matrices (see 2.8.1). Now  $B(X_0, X_1) \in M(133, \mathbf{Z}_{(5)}[X_0, X_1])$ , being the image of  $\exp(X_0 R_5 + (X_0^5/5 + X_1) R_5^5)$  under the homomorphism induced by  $X_0 \mapsto -X_0^5$  and  $X_1 \mapsto -X_1^5$  (also see 1.7). It follows from this, and 2.8.1, that  $A(X_0, X_1)$ ,  $A(X_0, X_1)^{-1} \in M(133, \mathbf{Z}_{(5)}[X_0, X_1])$ .

Let  $x = (x_0, x_1) \in W_2(\mathbb{C})$ . Substituting  $x$  for  $(X_0, X_1)$  in  $a(X_0, X_1)$  gives  $a(x) = x_0 N_r + (x_0^5/5 + x_1) H_5 \in \text{Der } L(\mathbb{C})$ . It then follows from 2.6.4 that

$$A(x) = \exp(a(x)) \in G(\mathbb{C}) = \text{Aut } L(\mathbb{C}).$$

We now transfer to  $K$ . Let  $y = (y_0, y_1) \in W_2(K)$ . Then

$$\bar{A}(X_0, X_1) = \bar{E}(X) \bar{B}(X_0, X_1) \bar{C}(X_0) \in M(133, K[X_0, X_1]).$$

Note that  $5\text{-nilp}(\bar{N}_r) = 5\text{-nilp}(\bar{R}_5) = 2$  and  $5\text{-nilp}(\bar{T}_5) = 1$ , by 2.8.1. Substituting  $y$  for  $(X_0, X_1)$  in  $\bar{A}(X_0, X_1)$  gives

$$\bar{A}(y) = e_5(\bar{N}_r, y) e_5(\bar{R}_5, (-y_0^5, -y_1^5)) e_5(\bar{T}_5, y_0^{25}).$$

Moreover  $\bar{A}(y) \in G(K) = \text{Aut } L(K)$ : argue as in the proof of 2.6.5 and [T1, Lemma 1]. Now define

$$W = \left\{ \hat{y} = (y; -y_0^5, -y_1^5; y_0^{25}) : y = (y_0, y_1) \in W_2(K) \right\} \subseteq W_2(K) \times W_2(K) \times W_1(K).$$

Let  $\pi : W_2(K) \rightarrow W_2(K)$  be the ring homomorphism, where  $(y_0, y_1) \mapsto (y_0^5, y_1^5)$ ; see p.18.

Define  $a = (-1, 0)$ ,  $z = (z_0, z_1) \in W_2(K)$ . Then  $ya = (-y_0, -y_1)$ , using (8) of chapter 1.

Now

$$\begin{aligned}\pi(y)a + \pi(z)a &= (\pi(y) + \pi(z))a \\ &= \pi(y+z)a.\end{aligned}$$

(Since 5 is *odd*, we have  $a = -1$ .) It follows that  $W \cong W_2(K)$ , under the map  $W_2(K) \rightarrow W$  sending  $y \mapsto \hat{y}$ . By 1.6.4 we have the following morphisms of algebraic groups:

$$(*) \quad \begin{array}{ccc} W_2(K) & \rightarrow & SL(133, K) \\ y & \mapsto & e_5(\bar{N}_r, y) \end{array} \quad \begin{array}{ccc} W_2(K) & \rightarrow & SL(133, K) \\ y & \mapsto & e_5(\bar{R}_5, y) \end{array} \quad \begin{array}{ccc} W_1(K) & \rightarrow & SL(133, K) \\ y_0 & \mapsto & e_5(\bar{T}_5, y_0) \end{array}$$

(actually isomorphisms onto their images). Consider the map

$$\begin{aligned}\phi : W &\rightarrow SL(133, K) \\ \hat{y} &\mapsto \bar{A}(y)\end{aligned}$$

Define  $V_r = \text{Im } \phi \subseteq G(K)$ . Then  $\phi$  is a morphism of varieties (argue as in the proof of 2.7.6). Since  $\bar{N}_r$ ,  $\bar{R}_5$ , and  $\bar{T}_5$  are mutually commuting matrices, it follows from  $(*)$  that  $\phi$  is a homomorphism of groups. At this stage the arguments used in the proof of 2.7.6 do not transfer nicely to this case. Instead we argue directly: Write  $A = (A_{ij}) = A(X_0, X_1)$  for brevity, where  $1 \leq i, j \leq 133$  (so  $A = \exp(X_0 N_r + (X_0^5/5 + X_1) H_5)$ ). Using Appendix C we obtain  $\text{ht}(N_r) = 1$  and  $\text{ht}(N_r^5) = \text{ht}(H_5) = 6$ . The  $(1, 2)$ -th entry of  $N_r$  is 1. The  $(1, 7)$ -th entry of  $N_r^5$  is 1. The  $(1, 7)$ -th entry of  $H_5$  is  $-4$ . Moreover the  $(1, 7)$ -th entry of  $N_r^i$  is 0 for  $1 \leq i \leq 4$ . It follows that

$$\begin{aligned}A_{12} &= X_0 \\ A_{17} &= -19X_0^5/24 - 4X_1\end{aligned}$$

Now write  $\bar{A}(y) = (\bar{A}_{ij})$ , where  $1 \leq i, j \leq 133$ . The calculations above imply that

$$(*) \quad \begin{aligned}\bar{A}_{12} &= y_0 \\ \bar{A}_{17} &= -y_0^5 + y_1\end{aligned}$$

We now show that  $\phi$  is injective: Let  $\hat{y} \in \ker \phi$  (where  $y = (y_0, y_1) \in W_2(K)$ ), so that  $\bar{A}(y) = \bar{I}$ . Then  $(*)$  gives  $y_0 = y_1 = 0$ , and so  $\hat{y} = 0$  as required. It also follows from  $(*)$  that the inverse map  $\phi^{-1} : V_r \rightarrow W$  is a morphism of varieties. Therefore  $\phi : W \rightarrow V_r$  is an isomorphism of algebraic groups. Now by 2.8.3,  $V_r$  contains a regular unipotent element  $v$  (take  $y_0 \neq 0$ ), where  $\text{o}(v) = 5^2$  (see 1.2.3(c)), giving the result in this case.

For the cases  $p = 7, 11, 13, 17$  and  $p = 19, 23, 29, 31$  we can use the arguments for the corresponding cases in the proof of 2.7.6. For  $p > 31$  argue as in the proof of 2.6.7.  $\square$

## 2.9 The Adjoint Case

In this section we consider the case where  $\overline{G}$  is a simple algebraic group of *adjoint* type. Combining the main results of sections 2.2 – 2.8, gives the following

**Theorem 2.9.1** *Let  $\overline{G}$  be a simple adjoint algebraic group, other than  $\overline{G} = E_8$ , defined over an algebraically closed field  $K$  of good characteristic  $p > 0$ . Then the following hold:*

- (i) *Let  $\bar{u} \in \overline{G}_u$  be a regular unipotent element, and suppose  $o(\bar{u}) = p^t$ , for some  $t \in \mathbb{N}$ . Then there exists a closed subgroup  $\overline{V}$  of  $\overline{G}$ , with  $\overline{V} \cong W_t(K)$  and  $\bar{u} \in \overline{V}$ .*
- (ii) *Suppose  $\overline{G} = E_7$ , and let  $\bar{v} \in \overline{G}_u$  be a subregular unipotent element, with  $o(\bar{v}) = p^s$ , for some  $s \in \mathbb{N}$ . Then there exists a closed subgroup  $\overline{W}$  of  $\overline{G}$ , with  $\overline{W} \cong W_s(K)$  and  $\bar{v} \in \overline{W}$ .*

**Proof** Let  $G$  be one of the groups in the table below:

Type	$A_l, l \geq 1$	$B_l, l \geq 2$	$C_l, l \geq 3$	$D_l, l \geq 4$
$G$	$SL(l+1, K)$	$SO(2l+1, K)$	$Sp(2l, K)$	$SO(2l, K)$
Isogeny Class	simply-connected	adjoint	simply-connected	neither

Type	$E_7$	$F_4$	$G_2$	
$G$	$\text{Aut } L(K)$	$\text{Aut } \mathcal{J}(K)$	$\text{Aut } \mathcal{C}(K)$	
Isogeny Class	adjoint	both	both	

Write  $Z = Z(G)$ . There exists a central isogeny

$$\begin{array}{ccc} \pi : G & \rightarrow & \overline{G} = G_{ad} \\ x & \mapsto & \bar{x} \end{array},$$

with  $\ker \pi = Z$ . See [Bo,22], [BT,2], and [Ti,1.2;1.5;2.6] for more details (if we further assume that  $p \nmid (l+1)$  in type  $A_l$ , then our restrictions on  $p$  imply that  $\overline{G} \cong G/Z$ ). The following

facts are readily verified:

- (1)  $\text{rk}(G) = \text{rk}(\overline{G})$
- (2)  $\dim Z_G(u) = \dim Z_{\overline{G}}(\overline{u})$ , for all  $u \in G_u$
- (3)  $\text{o}(u) = \text{o}(\overline{u})$ , for all  $u \in G_u$

(use the Jordan decomposition in  $G$ , combined with the fact that  $Z$  is finite, and consists entirely of semisimple elements). Now let  $u \in G_u$  be a regular unipotent element, and suppose  $\text{o}(u) = p^t$ , for some  $t \in \mathbb{N}$ . Then  $\overline{u}$  is a regular unipotent element of  $\overline{G}$ , with  $\text{o}(\overline{u}) = p^t$  (by (1), (2), and (3)). From the main results of 2.2 – 2.8, we have  $u \in V$ , a closed subgroup of  $G$ , isomorphic to  $W_t(K)$ . Write  $\phi = \pi|_V$  and  $\overline{V} = \pi(V)$ , a closed subgroup of  $\overline{G}$ . It follows from [Bo,22.4] that  $\phi : V \rightarrow \overline{V}$  is an *isomorphism* of algebraic groups. Therefore  $\overline{u} \in \overline{V} \cong V \cong W_t(K)$  (when  $\overline{G} \cong G/Z$ , we can alternatively use [Bo,6.12] and [Sp3,4.3.4]).

The subregular unipotent elements in type  $\overline{G} = E_7$  have already been dealt with in 2.8.5(ii). Finally suppose  $\overline{G} = E_6$ , then we have a natural embedding  $F_4 \subseteq E_6$ , where the  $F_4$  is the fixed point subgroup of the graph automorphism of  $E_6$ . Moreover the regular unipotent elements of  $F_4$  are also regular in  $E_6$ , and so the result follows in this case also (see [C1,13], [T2], and [T3,5] for more details).  $\square$

It is worth noting that we have a natural embedding  $B_{l-1} \subseteq D_l$ , where the  $B_{l-1}$  is the fixed point subgroup of the involutory graph automorphism of  $D_l$ . Moreover, this subgroup contains a regular unipotent element of  $D_l$ . It follows that we can avoid the case  $D_l$  altogether; however we have included it in 2.5 for completeness. See [T2,p.70] and [SSz,p.5] for more details.

See 2.2 – 2.8 for the various orders of the regular and subregular elements given in 2.9.1.



## Chapter 3

# Reductive Algebraic Groups

In this chapter we extend our results on simple algebraic groups to reductive algebraic groups. Our aim is to prove the generalized problem stated on p.3 (under certain restrictions). We now restate this in the form of the following theorem:

**Main Theorem (MT)** *Let  $G$  be a reductive algebraic group defined over an algebraically closed field  $K$  of good characteristic  $p > 0$ . If  $G'$  contains a simple component of type  $E_8$ , further impose the restriction  $p > 29$ . Let  $1 \neq u \in G_u$  be unipotent, with  $\text{o}(u) = p^t$ , for some  $t \in \mathbb{N}$ . Then there exists a closed subgroup  $V$  of  $G$ , with  $V \cong W_t(K)$  and  $u \in V$ .*

For more details on the restriction on simple components of type  $E_8$ , see the remarks after 3.3.3 to follow.

In order to prove the MT, we will have to consider *arbitrary* unipotent elements, as opposed to just the regular and subregular classes. In 3.1 we study this problem for the various classical groups. This is followed by the general case in 3.2, culminating in a proof of the MT in 3.3.

### 3.1 The Cayley Transform

This section uses ideas from 1.3 (The Functional Equation Lemma), which should be consulted for more details. Let  $R$  be a commutative ring with identity,  $1 \in R$ , and suppose  $2 = 1 + 1$  is invertible in  $R$ . The following notation will be used: Let  $f(T) = \sum_{n=0}^{\infty} a_n T^n \in R[[T]]$ , and suppose  $a_0$  is invertible in  $R$ . Then  $f(T)$  has a *multiplicative* inverse, which we denote by  $1/f(T) \in R[[T]]$ , satisfying  $f(T)(1/f(T)) = (1/f(T))f(T) = 1 \in R$  (see [Ha,A.1.10]). Now define

$$R[[T]]_* = \left\{ f(T) = \sum_{n=0}^{\infty} a_n T^n \in R[[T]] : 1 + a_0 \text{ is invertible in } R \right\}.$$

Clearly  $R[[T]]_0 \subseteq R[[T]]_*$ . Given  $f(T) = \sum_{n=0}^{\infty} a_n T^n \in R[[T]]_*$ , we shall write

$$f^\gamma(T) = \frac{(1 - f(T))}{(1 + f(T))}.$$

If  $f^\gamma(T) = \sum_{n=0}^{\infty} b_n T^n$ , then  $1 + b_0 = 1 + (1 - a_0)(1 + a_0)^{-1}$ , which is invertible in  $R$ , with inverse  $(1 + a_0)/2$ . This determines a map

$$\begin{aligned} \gamma : R[[T]]_* &\rightarrow R[[T]]_* \\ f(T) &\mapsto f^\gamma(T) \end{aligned},$$

which is a type of *Cayley transform*. It is easy to see that  $\gamma^2 = 1$ . The following property is also clear: Let  $f(T) \in R[[T]]_*$  and  $g(T) \in R[[T]]_0$ , then

$$(*_1) \quad (f \circ g)^\gamma(T) = (f^\gamma \circ g)(T).$$

Now consider the case where  $R = \mathbb{Q}$  and  $f(T) = \exp(T) \in \mathbb{Q}[[T]]_*$ . If we define

$$\tanh(T) = \frac{\exp(2T) - 1}{\exp(2T) + 1} \in \mathbb{Q}[[T]]_0,$$

then  $\exp^\gamma(T) = -\tanh(T/2)$ . Recall the following definition: Let  $p$  be a fixed *odd* prime in  $\mathbb{N}$ . Then  $d(X, T) = \sum_{i=0}^{\infty} d(X)_i T^{p^i}$ , where each  $d(X)_i \in \mathbb{Q}[X] = \mathbb{Q}[X_0, X_1, X_2, \dots]$  are as in (23) of chapter 1. Let  $1 = (1, 0, 0, \dots) \in W(\mathbb{Q})$ , then substituting  $1$  for  $X = (X_0, X_1, X_2, \dots)$  in  $d(X, T)$  gives  $d(1, T) = \sum_{i=0}^{\infty} T^{p^i}/p^i \in \mathbb{Q}[[T]]_0$ . Now let  $h(T) \in \mathbb{Q}[[T]]_0$ . It then follows from  $(*_1)$  that

$$(*_2) \quad \gamma(\exp(d(1, h(T)))) = -\tanh(d(1, h(T))/2)$$

(these facts use the properties of composition, as stated on p.24).

We now obtain the inverse function power series of  $\tanh(T)$  (which clearly exists). Write  $f(T) = \tanh^{-1}(T)$ , then

$$T = \tanh(f(T)) = \frac{\exp(2f(T)) - 1}{\exp(2f(T)) + 1} \Rightarrow \exp(2f(T)) = \frac{1+T}{1-T}.$$

Therefore  $f(T) = 2^{-1} \log((1+T)/(1-T)) = 2^{-1}(\log(1+T) - \log(1-T))$  (see (18) of chapter 1, and [B1,IV,4.10]), and so

$$\tanh^{-1}(T) = \sum_{n=0}^{\infty} \frac{T^{2n+1}}{2n+1}$$

(see definition of  $l(T)$  on p.30). We have the following

**Lemma 3.1.1** *Let  $p$  denote an odd prime in  $\mathbb{N}$ . Then*

$$\exp(d(1, h(T))) = \frac{1-T}{1+T},$$

for some  $h(T) = \sum_{n=0}^{\infty} c_{2n+1} T^{2n+1} \in \mathbb{Z}_{(p)}[[T]]_0$ .

**Proof** Refer to 1.3, and take  $R = \mathbb{Q}$ ,  $S = \mathbb{Z}_{(p)}$ ,  $\sigma = 1$ , and  $r = 1/p$ . Then given  $g(T) = \sum_{n=1}^{\infty} b_n T^n \in \mathbb{Z}_{(p)}[[T]]_0$ , we define a new power series  $f_g(T) = \sum_{n=1}^{\infty} a_n T^n \in \mathbb{Q}[[T]]_0$  as follows: Write  $n = p^i m$ , where  $i \in \mathbb{N} \cup 0$ , and  $m \in \mathbb{N}$  with  $(m, p) = 1$ , then take

$$a_n = \begin{cases} b_n & : i = 0 \\ b_n + \frac{1}{p} a_{n/p} & : i \geq 1 \end{cases}$$

(see (16) of chapter 1). We then have  $d(1, T)/2 = f_g(T)$ , where  $g(T) = T/2 \in \mathbb{Z}_{(p)}[[T]]_0$  (note that  $1/2$  is invertible in  $\mathbb{Z}_{(p)}$ ), and  $-\tanh^{-1}(T) = f_{\bar{g}}(T)$ , where

$$\bar{g}(T) = \sum_{n=1}^{\infty} \bar{b}_n T^n \in \mathbb{Z}_{(p)}[[T]]_0 \quad \text{with} \quad \bar{b}_n = \begin{cases} -1/n & : n \text{ odd, } p \nmid n \\ 0 & : \text{otherwise} \end{cases}$$

(use induction on  $i$ ). Define  $h(T) = (f_g^{-1} \circ f_{\bar{g}})(T)$ . Since  $f_g(T) = d(1, T)/2$  involves no even powers of  $T$ , it follows that the same holds for  $f_g^{-1}(T)$ : Suppose not, then choose  $i \in \mathbb{N}$  minimal such that the coefficient of  $T^{2i}$  in  $f_g^{-1}(T)$  is non-zero; considering  $T = f_g(f_g^{-1}(T))$  then gives a contradiction. Moreover  $f_{\bar{g}}(T) = -\tanh^{-1}(T)$  is also of this form. Therefore 1.3.4(i) gives

$$h(T) = \sum_{n=0}^{\infty} c_{2n+1} T^{2n+1} \in \mathbb{Z}_{(p)}[[T]]_0.$$

Now  $(f_g^{-1} \circ (f_g \circ h))(T) = T$ , where  $f_g^{-1}(T) = (-\tanh^{-1})^{-1}(T) = -\tanh(T)$  (since  $\tanh^{-1}(T)$  involves no even powers of  $T$ ), and  $(f_g \circ h)(T) = d(1, h(T))/2$ . Thus  $-\tanh(d(1, h(T))/2) = T$ , and so  $(\ast_2)$  above gives

$$\gamma(\exp(d(1, h(T)))) = T.$$

The result follows by applying  $\gamma$  to both sides.  $\square$

We now transfer to a matrix setting, following [W,II,B,10]. Some properties of 1.7 are also used. Let  $p$  be a fixed *odd* prime in  $\mathbb{N}$ . For a finite set  $\Phi^+$ , let  $Y = (Y_\alpha : \alpha \in \Phi^+)$  be a set of indeterminates. Define (for  $n \geq 1$ )

$$M(n, \mathbb{Z}_{(p)}[Y])_\bullet = \left\{ M \in M(n, \mathbb{Z}_{(p)}[Y]) : \det(I_n + M) \text{ is invertible in } \mathbb{Z}_{(p)} \right\}.$$

Given  $M \in M(n, \mathbb{Z}_{(p)}[Y])_\bullet$ , we shall write

$$M^\gamma = (I_n - M)(I_n + M)^{-1},$$

for the Cayley transform of  $M$ . Rearranging this gives  $(I_n + M^\gamma)(I_n + M) = 2I_n$ , and so  $M^\gamma \in M(n, \mathbb{Z}_{(p)}[Y])_\bullet$ . The resulting map

$$\begin{array}{ccc} \gamma : M(n, \mathbb{Z}_{(p)}[Y])_\bullet & \rightarrow & M(n, \mathbb{Z}_{(p)}[Y])_\bullet \\ M & \mapsto & M^\gamma \end{array},$$

satisfies  $\gamma^2 = 1$ . Now let  $u \in U(n, \mathbb{Z}_{(p)}[Y]) \subseteq M(n, \mathbb{Z}_{(p)}[Y])_\bullet$ , and write  $e = (u - I_n)/2 \in u(n, \mathbb{Z}_{(p)}[Y])$ . Then

$$\begin{aligned} \gamma(u) &= (I_n - u)(I_n + u)^{-1} \\ &= -e(I_n + e)^{-1} \\ &= -e(I_n - e + e^2 - \dots + (-1)^{n-1}e^{n-1}) \\ &\in u(n, \mathbb{Z}_{(p)}[Y]). \end{aligned}$$

Now let  $X = (X_0, X_1, X_2, \dots)$  be another set of indeterminates. For the next result, we will need to work over the polynomial ring  $\mathbb{Q}[X, Y]$ .

**Lemma 3.1.2** [W,II,B,10,2.10.A], [C1,11.2.2] *Let  $A \in M(n, \mathbb{Z}_{(p)})$ ,  $n \in \mathbb{N}$ . Then the following hold:*

(i) Let  $u \in U(n, \mathbf{Z}_{(p)}[Y])$  and write  $N = \gamma(u)$ . If  $u^t A u = A$  then  $N^t A = -AN$ .

(ii) Let  $N \in u(n, \mathbf{Q}[X, Y])$  satisfy  $N^t A = -AN$ , and write  $E = \exp(N)$ . Then  $E^t A E = A$ .

Now fix  $u \in U(n, \mathbf{Z}_{(p)}[Y])$  and  $A \in M(n, \mathbf{Z}_{(p)})$ , and suppose  $u^t A u = A$ . Write  $N = \gamma(u) \in u(n, \mathbf{Z}_{(p)}[Y])$ , then  $N^t A = -AN$  by 3.1.2(i). Let  $h(T) = \sum_{i=0}^{\infty} c_{2i+1} T^{2i+1} \in \mathbf{Z}_{(p)}[[T]]_0$  be the power series arising in 3.1.1. Substituting  $N$  for  $T$  gives

$$N' = h(N) = \sum_{i=0}^{[(n-2)/2]} c_{2i+1} N^{2i+1} \in u(n, \mathbf{Z}_{(p)}[Y]).$$

Since  $N^t A = -AN$ , we have  $N'^t A = -AN'$ . Now recall  $d(X, T) = \sum_{i=0}^{\infty} d(X)_i T^i$ , and  $\exp(d(X, T)) = \sum_{i=0}^{\infty} c(X)_i T^i$  (see (23) of chapter 1). Substituting  $N'$  for  $T$  in  $d(X, T)$  gives  $d(X, N') \in u(n, \mathbf{Q}[X, Y])$ , and since  $p$  is odd, we have

$$d(X, N')^t A = -A d(X, N').$$

As in 1.7, we obtain

$$E(X, Y) = \exp(d(X, N')) = \sum_{i=0}^{n-1} c(X)_i N'^i \in U(n, \mathbf{Z}_{(p)}[X, Y]),$$

where by 3.1.2(ii),

$$(CT1) \quad E(X, Y)^t A E(X, Y) = A.$$

Let  $1 = (1, 0, 0, \dots) \in W(\mathbf{Q})$ . Substituting  $1$  for  $X$  in  $E(X, Y)$  gives  $E(1, Y) = \exp(d(1, N')) = \sum_{i=0}^{n-1} c(1)_i N'^i \in U(n, \mathbf{Z}_{(p)}[Y])$  (compare with 1.7). Now by 3.1.1,

$$\begin{aligned} \exp(d(1, N')) &= \exp(d(1, h(N))) \\ &= (I_n - N)(I_n + N)^{-1} \\ &= \gamma(N) \\ &= u, \end{aligned}$$

and so we have

$$(CT2) \quad u = \sum_{i=0}^{n-1} c(1)_i N'^i.$$

Now let  $K$  be a field of characteristic  $p$ . Let  $\psi : \mathbf{Z}_{(p)}[X, Y] \rightarrow K[X, Y]$  denote the natural homomorphism, and  $\psi_n : M(n, \mathbf{Z}_{(p)}[X, Y]) \rightarrow M(n, K[X, Y])$  the induced matrix

homomorphism. Write  $\overline{N'} = \psi_n(N')$ , then

$$\overline{E}(X, Y) = \psi_n(E(X, Y)) = \sum_{i=0}^{n-1} \overline{c}(X)_i \overline{N'}^i \in U(n, K[X, Y]),$$

where by (CT1),

$$(CT3) \quad \overline{E}(X, Y)^t \overline{A} \overline{E}(X, Y) = \overline{A},$$

where  $\overline{A} = \psi_n(A)$ . Now write  $\overline{u} = \psi_n(u)$ , then (CT2) gives

$$(CT4) \quad \overline{u} = \sum_{i=0}^{n-1} \overline{c}(\overline{I})_i \overline{N'}^i \in U(n, K[Y]),$$

where  $\overline{I} = (1, 0, 0, \dots) \in W(K)$ . For each  $\alpha \in \Phi^+$ , fix  $\lambda_\alpha \in K$ , and write  $\lambda = (\lambda_\alpha : \alpha \in \Phi^+)$ . Substituting  $\lambda$  for  $Y$  determines a ring homomorphism  $K[Y] \rightarrow K$ . Let  $N_\lambda$  and  $u_\lambda$  denote the images of  $\overline{N'}$  and  $\overline{u}$ , respectively, under the induced matrix homomorphism. If  $N_\lambda = 0$  then (CT4) implies  $u_\lambda = \overline{I}_n$ . Now suppose  $N_\lambda \neq 0$ , then  $p\text{-nilp}(N_\lambda) = t$ , for some  $t \in \mathbb{N}$ . We have

$$\overline{E}(X, \lambda) = \sum_{i=0}^{p^t-1} \overline{c}(X)_i N_\lambda^i \in U(n, K[X]),$$

where by (CT3),

$$(CT5) \quad \overline{E}(X, \lambda)^t \overline{A} \overline{E}(X, \lambda) = \overline{A}.$$

Note that  $\overline{c}(X)_i \in K[X_0, X_1, \dots, X_{t-1}]$ ,  $0 \leq i \leq p^t - 1$  (see 1.4.3(ii)). Now let  $y = (y_0, y_1, \dots, y_{t-1}) \in W_t(K)$ , then substituting  $y$  for  $X$  in  $\overline{E}(X, \lambda)$  gives

$$\overline{E}(y, \lambda) = \sum_{i=0}^{p^t-1} \overline{c}(y)_i N_\lambda^i = e_p(N_\lambda, y) \in U(n, K),$$

the Artin-Hasse exponential of  $N_\lambda$  with respect to  $y$ , as defined in (27) of chapter 1. From (CT5) we obtain

$$(CT6) \quad e_p(N_\lambda, y)^t \overline{A} e_p(N_\lambda, y) = \overline{A}.$$

It also follows from (CT4) that

$$(CT7) \quad u_\lambda = \sum_{i=0}^{p^t-1} \overline{c}(\overline{I})_i N_\lambda^i = e_p(N_\lambda, \overline{I}),$$

where  $\overline{I} = (1, 0, \dots, 0) \in W_t(K)$ .

We now come to the main result of this section (refer to 2.1, 2.3 – 2.5 for notation).

**Theorem 3.1.3** *Let  $K$  be an algebraically closed field of characteristic  $p > 2$ . Suppose  $G = SO(2l+1, K)$ ,  $Sp(2l, K)$ , or  $SO(2l, K)$ , where  $l \geq 2, 3$ , or  $4$ , respectively. Let  $1 \neq v \in G_u$  be unipotent, and suppose  $\text{o}(v) = p^t$ , for some  $t \in \mathbb{N}$ . Then there exists a closed subgroup  $V$  of  $G$ , with  $V \cong W_t(K)$  and  $v \in V$ .*

**Proof** Let  $n = 2l+1, 2l$ , or  $2l$ , where  $l \geq 2, 3$ , or  $4$ , respectively. As usual, we view  $G$  as a Chevalley group (see 2.3 – 2.5). Let  $L$  be the complex simple Lie algebra corresponding to  $G$ , and  $A \in M(n, \mathbb{Z})$  the matrix representing the form associated with  $L$  (so  $x^t A = -Ax$  for all  $x \in L$ ). Since the maximal connected unipotent subgroups of  $G$  are all conjugate, we can restrict our attention to  $U = \langle X_\alpha : \alpha \in \Phi^+ \rangle$ . Define

$$u = \prod_{\alpha \in \Phi^+} \exp(Y_\alpha e_\alpha) \in U(n, \mathbb{Z}[Y]),$$

where  $Y = (Y_\alpha : \alpha \in \Phi^+)$ . Note that  $u^t A u = A$  (see 3.1.2(ii)). For each  $\alpha \in \Phi^+$ , fix  $\lambda_\alpha \in K$ , and write  $\lambda = (\lambda_\alpha : \alpha \in \Phi^+)$ . Define  $N_\lambda$  and  $u_\lambda$  as above. We have

$$u_\lambda = \prod_{\alpha \in \Phi^+} x_\alpha(\lambda_\alpha) \in U.$$

Suppose  $N_\lambda \neq 0$  (so that  $u_\lambda \neq 1$ ), then  $p\text{-nilp}(N_\lambda) = t$ , for some  $t \in \mathbb{N}$ . Consider the map

$$\begin{aligned} \phi : W_t(K) &\rightarrow SL(n, K) \\ y &\mapsto e_p(N_\lambda, y) \end{aligned}.$$

By (CT6) above, we have  $V = \phi(W_t(K)) \subseteq G$ . Now by 1.6.4,  $\phi : W_t(K) \rightarrow V$  is an isomorphism of algebraic groups. Let  $1 = (1, 0, \dots, 0) \in W_t(K)$ , then (CT7) gives

$$u_\lambda = \phi(1) \in V.$$

Moreover, by 1.2.3(c), we have  $\text{o}(u_\lambda) = \text{o}(1) = p^t$ . The result follows.  $\square$

A similar (easier) argument gives the same result in the case  $G = SL(l+1, K)$ ,  $l \geq 1$ , where  $K$  is an algebraically closed field of characteristic  $p > 0$ . We omit most of the details, but prove the analogue of the key result 3.1.1. The Cayley transform is replaced by the simpler map

$$\begin{aligned} \gamma : \mathbb{Q}[X][[T]] &\rightarrow \mathbb{Q}[X][[T]] \\ f(T) &\mapsto 1 - f(T) \end{aligned},$$

which clearly satisfies  $\gamma^2 = 1$ . We have the following

**Lemma 3.1.4** *Let  $p$  be a fixed prime in  $\mathbb{N}$ . Then*

$$\exp(d(1, h(T))) = 1 - T,$$

*for some  $h(T) \in \mathbb{Z}_{(p)}[[T]]_0$ .*

**Proof** Refer to 1.3, and take  $R = \mathbb{Q}$ ,  $S = \mathbb{Z}_{(p)}$ ,  $\sigma = 1$ , and  $r = 1/p$ . We have  $d(1, T) = f_g(T)$ , where  $g(T) = T \in \mathbb{Z}_{(p)}[[T]]_0$ . Now  $\gamma(\exp(T)) = -\sum_{n=1}^{\infty} T^n/n!$ , which has as its inverse function power series  $l(-T) = \log(1 - T) = -\sum_{n=1}^{\infty} T^n/n$ . We have  $l(-T) = f_{\bar{g}}(T)$ , where

$$\bar{g}(T) = \sum_{n=1}^{\infty} \bar{b}_n T^n \in \mathbb{Z}_{(p)}[[T]]_0 \quad \text{with} \quad \bar{b}_n = \begin{cases} -1/n & : p \nmid n \\ 0 & : \text{otherwise} \end{cases}.$$

Then  $h(T) = (f_g^{-1} \circ f_{\bar{g}})(T) \in \mathbb{Z}_{(p)}[[T]]_0$  by 1.3.4(i). Now  $(f_{\bar{g}}^{-1} \circ (f_g \circ h))(T) = T$ , where  $f_{\bar{g}}^{-1}(T) = 1 - \exp(T)$ , and  $(f_g \circ h)(T) = d(1, h(T))$ . Thus  $1 - \exp(d(1, h(T))) = T$ , and so the result follows by applying  $\gamma$  to both sides.  $\square$

Arguing as in the proof of 3.1.3, we obtain the following (refer to 2.2 for notation)

**Theorem 3.1.5** *Let  $K$  be an algebraically closed field of characteristic  $p > 0$ . Suppose  $G = SL(l + 1, K)$ , where  $l \geq 1$ . Let  $1 \neq u \in G_u$  be unipotent, and suppose  $o(u) = p^t$ , for some  $t \in \mathbb{N}$ . Then there exists a closed subgroup  $V$  of  $G$ , with  $V \cong W_t(K)$  and  $u \in V$ .*

For the various orders of the unipotent elements in the classical groups, consult the ‘order formula’ in [T2, 3.4].



## 3.2 Semiregular Unipotent Elements

In 3.1, for the classical groups, we extended the results of the previous chapter to include *every* unipotent class. However it is not clear how the methods used in 3.1 can be applied to the various exceptional groups. In this section we present an alternative strategy for solving the MT.

Let  $G$  be a simple *adjoint* algebraic group defined over an algebraically closed field  $K$  of *good* characteristic  $p > 0$  (note that  $Z(G) = 1$ ). Let  $G_s$  denote the set of semisimple elements of  $G$ . A unipotent element  $u \in G_u$  is said to be *semiregular* if the following condition holds:

$$s \in G_s \cap Z_G(u) \Rightarrow s = 1.$$

We shall omit the case  $G = E_8$ , but see the remarks after 3.3.3 to follow. Every regular unipotent element is semiregular (see 2.1). These elements have been dealt with in 2.9.1. Now suppose  $u \in G_u$  is *not* semiregular. Then there exists  $1 \neq s \in G_s \cap Z_G(u)$ , and so  $u \in Z_G(s)$ . This forces  $u \in Z_G(s)^\circ$ , a *proper* closed (connected) *reductive* subgroup of  $G$  (see [C2,3.5] and [H3,1.12;2.2]). For details on the root system of  $(Z_G(s)^\circ)'$ , consult [BdS], [C2,3.5.4], and [H3,2.12–2.15]. Therefore, in an inductive sense, we can restrict our attention to the non-regular semiregular unipotent elements of  $G$ .

Since  $p$  is good, non-regular semiregular unipotent elements only occur in the following cases:  $G = D_l$ ,  $l \geq 4$ ,  $E_6$ ,  $E_7$  (and  $E_8$ , which we are not considering). See [SS,III,4.28;IV,2.30] and [C2,5.11] for more details. In type  $D_l$ , there are  $[(l-2)/2]$  such classes, labelled  $D_l(a_r)$ ,  $1 \leq r \leq [(l-2)/2]$ , in Bala-Carter notation. Given  $u_r \in D_l(a_r)$ , it is shown in [T2,3.2] that  $u_r$  lies in a (proper) closed reductive subgroup of  $D_l$  of type  $B_r \times B_{l-r-1}$ . In any case, we have dealt with type  $D_l$ , for *all* unipotent elements, in 3.1.3. When  $G = E_6$ , there is only one non-regular semiregular class, which is denoted by  $E_6(a_1)$ . It is the class of subregular unipotent elements of  $E_6$ . Given  $u_1 \in E_6(a_1)$ , it is shown in [T2,2.7] that  $u_1$  lies in a (proper) closed reductive subgroup of  $E_6$  of type  $C_4$ . This leaves the case  $G = E_7$ , in which there are two such classes, labelled  $E_7(a_1)$  and  $E_7(a_2)$ . These are, respectively, the classes of subregular and 2-regular unipotent elements of  $E_7$ . The first of these classes has been dealt with in 2.9.1(ii). Now let  $u_2 \in E_7(a_2)$ . Then  $u_2$  lies in a (proper) closed reductive

subgroup of  $E_7$  of type  $A_1 \times F_4$  : For  $p > 11$  this follows from [LT]. When  $p = 5, 7$ , and  $11$ , the tables of Jordan blocks and  $p^{th}$ -powers of unipotent classes given in [La], combined with [Sz,1.9], can be used to show that a regular element of the  $A_1 \times F_4$  subgroup lies in the class  $E_7(a_2)$ .

We summarize this information in the table below:

$G$	Class $\mathcal{C}$	Overgroup of $u \in \mathcal{C}$
$D_l$	$D_l(a_r)$	$B_r \times B_{l-r-1}$ , $1 \leq r \leq [(l-2)/2]$
$E_6$	$E_6(a_1)$	$C_4$
$E_7$	$E_7(a_2)$	$A_1 \times F_4$

It is worth noting that the regular unipotent elements of 2.2 – 2.8, along with the sub-regular unipotent elements of 2.8, *cannot* in general be embedded in proper closed reductive subgroups. This can be seen from the following observation, which was pointed out to the author by R. Lawther: Let  $1 \neq u \in G_u$ , with  $G \neq A_1$ . If  $o(u) = p$  then by [T2,4.1],  $u$  lies in a proper closed reductive subgroup of  $G$  of type  $A_1$ , so assume  $o(u) > p$ . Suppose  $u \in H \subsetneq G$ , a proper closed reductive subgroup. Then  $u \in H' = X_1 \cdots X_n$ , where the  $X_i$ ,  $1 \leq i \leq n$ , are the simple components of  $H'$  (see [H2,27.5]). Write  $u = x_1 \cdots x_n$ ,  $x_i \in X_i$ , then without loss of generality,  $x_1^p \neq 1$ , since  $u^p \neq 1$ . Note that  $X_1 \neq A_1$ . Therefore  $x_1 \in X_1 \subsetneq G$ , a proper closed simple subgroup of  $G$  with  $\text{rk}(X_1) \geq 2$ . However this is *not* always possible: For example, take  $G = E_7$ ,  $p = 13$ , and  $u_1 \in E_7(a_1)$ . Then  $o(u_1) = 13^2$ . Using [LS,Table 8.2], we see that there are *no* proper simple subgroups of  $G$  containing unipotent elements of order  $> 13$ .

When considering the regular unipotent elements above, we can also use [SSz]. Indeed let  $G$  be of type  $G_2$ ,  $F_4$ , or  $E_7$ . Let  $u \in G_u$  be regular with  $o(u) = p^2$  (so  $p < \text{ht}(r_0) + 1$ ). Using [SSz,Theorem A], we see that there are *no* proper closed reductive subgroups of  $G$  containing  $u$ .

In the next section we consider the case of an arbitrary reductive algebraic group.

### 3.3 The Main Theorem

In this section we prove the main theorem MT, as stated on p.113. We begin with a few (well-known) remarks on the decomposition of reductive algebraic groups. Let  $G$  be a reductive algebraic group defined over an algebraically closed field  $K$  of characteristic  $p > 0$ , and suppose  $G_u \neq 1$ . Write  $Z = Z(G)$ . Then  $G = G'Z^\circ$ , where  $1 \neq G' = (G, G)$  is a connected semisimple algebraic group, and  $Z^\circ = R(G)$  is a torus (moreover the group  $G' \cap Z^\circ$  is finite). In turn a connected semisimple algebraic group can be broken down into an *almost* direct product of simple algebraic groups (see [H2,19.5;27.5]).

The main theorem (3.3.3) will follow from the following two lemmas.

**Lemma 3.3.1** *Let  $G$  be a connected semisimple algebraic group of adjoint type defined over an algebraically closed field of characteristic  $p > 0$ . Suppose we have established the MT for simple adjoint algebraic groups. Then the MT also holds for  $G$ .*

**Proof** Every connected semisimple adjoint algebraic group is in a unique way isomorphic to a *direct* product of simple adjoint algebraic groups (see [Ti,3]). By induction it will suffice to consider the case  $G = G_1 \times G_2$ , where  $G_i$ ,  $i = 1, 2$ , is a simple adjoint algebraic group. Let  $1 \neq u \in G_u$  and suppose  $o(u) = p^t$ , for some  $t \in \mathbb{N}$ . Then  $u = (u_1, u_2)$  where  $u_i \in (G_i)_u$ , and (without loss of generality)  $o(u_1) = p^t$  and  $o(u_2) = p^s$ ,  $0 \leq s \leq t$ . If  $s = 0$  we are done, so assume  $1 \leq s \leq t$ . By assumption we have  $u_i \in V_i$ , a closed subgroup of  $G_i$ , with isomorphisms (of algebraic groups)

$$\phi_1 : V_1 \rightarrow W_t(K) \quad \text{and} \quad \phi_2 : V_2 \rightarrow W_s(K).$$

Write  $x_i = \phi_i(u_i)$ ,  $i = 1, 2$ . By 1.2.5 there exists a morphism of algebraic groups

$$\psi : W_t(K) \rightarrow W_s(K)$$

satisfying  $\psi(x_1) = x_2$ . Consider the following composition

$$V_1 \xrightarrow{\phi_1} W_t(K) \xrightarrow{\psi} W_s(K) \xrightarrow{\phi_2^{-1}} V_2.$$

Set  $\phi = \phi_2^{-1} \circ \psi \circ \phi_1$ , then  $\phi : V_1 \rightarrow V_2$  is a morphism of algebraic groups satisfying  $\phi(u_1) = u_2$ .

Now define

$$V = \{(x, \phi(x)) : x \in V_1\} \stackrel{\text{closed}}{\subseteq} G.$$

We have  $u \in V$ . The map

$$\begin{aligned}\pi : V_1 &\rightarrow V \\ x &\mapsto (x, \phi(x))\end{aligned}$$

is clearly a bijective morphism of algebraic groups. The inverse  $\pi^{-1}$ , being projection onto the first factor, is a morphism of varieties, and so  $\pi$  is an *isomorphism* of algebraic groups, as required.  $\square$

The final lemma is a type of ‘lifting’ argument.

**Lemma 3.3.2** *Let  $G$  be an arbitrary connected semisimple algebraic group defined over an algebraically closed field  $K$  of characteristic  $p > 0$ . Suppose the MT holds for the corresponding adjoint group  $G_{ad}$ . Then the MT also holds for  $G$ .*

**Proof** Write  $Z = Z(G)$ . There exists a central isogeny

$$\begin{aligned}\pi : G &\rightarrow \bar{G} = G_{ad} \\ x &\mapsto \bar{x}\end{aligned},$$

with  $\ker \pi = Z$ ; see [BT,2.26] and [Ti,2.6.1] for more details. (Suppose  $G_1, \dots, G_n$  are the simple components of  $G$ . If  $p$  is good for each  $G_i$ , and  $p \nmid (l+1)$  if some  $G_j$  has type  $A_l$ , then we have  $\bar{G} \cong G/Z$ .) Let  $1 \neq u \in G_u$  and suppose  $\text{o}(u) = p^t$ , for some  $t \in \mathbb{N}$ . Then  $\bar{u}$  is unipotent, with  $\text{o}(\bar{u}) = p^t$ , since  $\ker \pi = Z$  consists entirely of semisimple elements. By assumption  $\bar{u} \in \bar{V}$ , a closed subgroup of  $\bar{G}$ , with  $\bar{V} \cong W_t(K)$ . Using [Bo,22.4] and [H2,21.3C], we can choose a maximal connected unipotent subgroup  $U$  of  $G$  such that  $\phi = \pi|_U : U \rightarrow \pi(U)$  is an *isomorphism* of algebraic groups, and  $\bar{V} \subseteq \pi(U)$ . Moreover  $\pi(u) = \bar{u} \in \pi(U)$ , which forces  $u \in U$ , using the Jordan decomposition in  $G$ , and the fact that  $\ker \pi = Z$ . Write  $V = \phi^{-1}(\bar{V})$ , a closed subgroup of  $G$ . Then  $u \in V \cong \bar{V} \cong W_t(K)$ , as required.  $\square$

Note that 3.3.2 extends at once to an arbitrary (connected) reductive group  $G$  (the Jordan decomposition in  $G$  gives  $G_u \subseteq G'$ , and so we can work entirely within the connected semisimple subgroup  $G'$ ). A slightly different approach which yields the same results is as follows: Assuming the MT holds for simple adjoint groups, establish the result for arbitrary simple groups (arguing as in 3.3.2). Now let  $G$  be an arbitrary (connected) semisimple group, with simple components  $G_1, \dots, G_n$ . Then the canonical map  $\pi : G_1 \times \dots \times G_n \rightarrow G$  is a

central isogeny (see [Bo,14.10;22.9;22.10] and [H2,27.5]). Having established the result for  $G_1 \times \cdots \times G_n$  (arguing as in 3.3.1), we can then use [Bo,22.4] to deduce the result for  $G$ .

We can now prove the main theorem:

**Theorem 3.3.3** (The Main Theorem) *Let  $G$  be a reductive algebraic group defined over an algebraically closed field  $K$  of good characteristic  $p > 0$ . Assume  $G_u \neq 1$ , and that  $G'$  has no simple component of type  $E_8$ . Let  $1 \neq u \in G_u$  and suppose  $\text{o}(u) = p^t$ , for some  $t \in \mathbb{N}$ . Then there exists a closed subgroup  $V$  of  $G$ , with  $V \cong W_t(K)$  and  $u \in V$ .*

**Proof** We use induction on  $\dim(G)$ . The induction starts at  $\dim(G) = 3$ , where  $G$  is of type  $A_1$ . This is easy since the maximal connected unipotent subgroups are all 1-dimensional, and so isomorphic to  $W_1(K)$ . Now suppose  $\dim(G) > 3$ , and that the result holds for (connected) reductive groups  $H$  with  $\dim(H) < \dim(G)$ . By 3.3.1 and 3.3.2 we may assume that  $G$  is a simple adjoint algebraic group. Using section 3.2 (and induction) we can further reduce to the cases in the table below:

$G$	$A_l, l \geq 1$	$B_l, l \geq 2$	$C_l, l \geq 3$	$D_l, l \geq 4$	$E_7$	$F_4$	$G_2$
$u$	regular	regular	regular	regular	regular subregular	regular	regular

All of these cases have been dealt with in 2.9.1, and so the result follows.  $\square$

For reasons of space and time, we have been unable to include the case where  $G$  is a simple algebraic group of type  $E_8$ . However we observe the following: Let  $1 \neq u \in G_u$  be unipotent, and suppose  $p > 29$  (this condition is by no means thought to be necessary). It is shown in [T2,2.2;4.1] that  $\text{o}(u) = p$ , and  $u$  lies in a closed reductive subgroup of  $G$  of type  $A_1$ . In particular  $u \in V$ , a closed subgroup of  $G$ , with  $V \cong W_1(K)$ . It then follows that 3.3.3 holds for *all* reductive algebraic groups, subject to this prime restriction on any simple components of type  $E_8$  (with  $p$  good for the remaining components).

### 3.4 Appendix A

This section contains some calculations needed for type  $G_2$  (see 2.6). Write  $\alpha_3 = \alpha_1 + \alpha_2$ ,  $\alpha_4 = 2\alpha_1 + \alpha_2$ ,  $\alpha_5 = 3\alpha_1 + \alpha_2$ , and  $\alpha_6 = 3\alpha_1 + 2\alpha_2$ . Then a typical element of  $U = \langle X_\alpha : \alpha \in \Phi^+ \rangle$  is, for  $\mu_i \in K$ ,  $1 \leq i \leq 6$ ,

$$\prod_{i=1}^6 x_{\alpha_i}(\mu_i) = \begin{bmatrix} (1, 1, 1) \\ (1, 2, \mu_1) \\ (1, 3, -\mu_1\mu_2 - \mu_3) \\ (1, 4, 2\mu_1\mu_3 + 2\mu_4) \\ (1, 5, \mu_1\mu_4 + \mu_5) \\ (1, 6, \mu_1\mu_2\mu_4 - \mu_1\mu_3^2 + \mu_3\mu_4 + \mu_6) \\ (1, 7, \mu_1\mu_2\mu_5 - 2\mu_1\mu_3\mu_4 - \mu_1\mu_6 + \mu_3\mu_5 - \mu_4^2) \\ (2, 2, 1) \\ (2, 3, -\mu_2) \\ (2, 4, 2\mu_3) \\ (2, 5, \mu_4) \\ (2, 6, \mu_2\mu_4 - \mu_3^2) \\ (2, 7, \mu_2\mu_5 - 2\mu_3\mu_4 - \mu_6) \\ (3, 3, 1) \\ (3, 4, 2\mu_1) \\ (3, 5, -\mu_1^2) \\ (3, 6, -\mu_1^2\mu_2 - 2\mu_1\mu_3 - \mu_4) \\ (3, 7, -\mu_1^2\mu_3 - 2\mu_1\mu_4 - \mu_5) \\ (4, 4, 1) \\ (4, 5, -\mu_1) \\ (4, 6, -\mu_1\mu_2 - \mu_3) \\ (4, 7, -\mu_1\mu_3 - \mu_4) \\ (5, 5, 1) \\ (5, 6, \mu_2) \\ (5, 7, \mu_3) \\ (6, 6, 1) \\ (6, 7, -\mu_1) \\ (7, 7, 1) \end{bmatrix}$$

(where  $(i, j, k)$  means the  $(i, j)$ -th entry is  $k$ ; entries not present are zero).

Let  $N = e_{\alpha_1} + e_{\alpha_2} = e_{12} - e_{23} + 2e_{34} - e_{45} + e_{56} - e_{67} \in M(7, \mathbb{C})$ . Write  $A_5(X) = \exp(X_0 N + (X_0^5/5 + X_1)N^5)$  and  $A_p(X) = \exp(X_0 N)$ , where  $p > 5$ . Then we have

$$\begin{array}{ll}
 A_5(X) = \begin{bmatrix} (1, 1, 1) \\ (1, 2, X_0) \\ (1, 3, -X_0^2/2) \\ (1, 4, -X_0^3/3) \\ (1, 5, X_0^4/12) \\ (1, 6, 5X_0^5/12 + 2X_1) \\ (1, 7, -29X_0^6/72 - 2X_0X_1) \\ (2, 2, 1) \\ (2, 3, -X_0) \\ (2, 4, -X_0^2) \\ (2, 5, X_0^3/3) \\ (2, 6, X_0^4/12) \\ (2, 7, -5X_0^5/12 - 2X_1) \\ (3, 3, 1) \\ (3, 4, 2X_0) \\ (3, 5, -X_0^2) \\ (3, 6, -X_0^3/3) \\ (3, 7, X_0^4/12) \\ (4, 4, 1) \\ (4, 5, -X_0) \\ (4, 6, -X_0^2/2) \\ (4, 7, X_0^3/6) \\ (5, 5, 1) \\ (5, 6, X_0) \\ (5, 7, -X_0^2/2) \\ (6, 6, 1) \\ (6, 7, -X_0) \\ (7, 7, 1) \end{bmatrix} & A_p(X) = \begin{bmatrix} (1, 1, 1) \\ (1, 2, X_0) \\ (1, 3, -X_0^2/2) \\ (1, 4, -X_0^3/3) \\ (1, 5, X_0^4/12) \\ (1, 6, X_0^5/60) \\ (1, 7, -X_0^6/360) \\ (2, 2, 1) \\ (2, 3, -X_0) \\ (2, 4, -X_0^2) \\ (2, 5, X_0^3/3) \\ (2, 6, X_0^4/12) \\ (2, 7, -X_0^5/60) \\ (3, 3, 1) \\ (3, 4, 2X_0) \\ (3, 5, -X_0^2) \\ (3, 6, -X_0^3/3) \\ (3, 7, X_0^4/12) \\ (4, 4, 1) \\ (4, 5, -X_0) \\ (4, 6, -X_0^2/2) \\ (4, 7, X_0^3/6) \\ (5, 5, 1) \\ (5, 6, X_0) \\ (5, 7, -X_0^2/2) \\ (6, 6, 1) \\ (6, 7, -X_0) \\ (7, 7, 1) \end{bmatrix}
 \end{array}$$

### 3.5 Appendix B

This section contains some calculations needed for type  $F_4$  (see 2.7). We begin with the images of the various  $T \in D_4$ , arising on p.97, under the triality automorphisms  $\psi$  and  $\phi$ .

$T$	$T^\psi$	$T^\phi$
$E_{23} - E_{76}$	$E_{23} - E_{76}$	$E_{23} - E_{76}$
$-E_{52} + E_{61}$	$-E_{47} + E_{38}$	$-E_{47} + E_{38}$
$-E_{53} + E_{71}$	$E_{46} - E_{28}$	$E_{46} - E_{28}$
$E_{12} - E_{65}$	$E_{12} - E_{65}$	$E_{12} - E_{65}$
$E_{13} - E_{75}$	$E_{13} - E_{75}$	$E_{13} - E_{75}$
$-E_{63} + E_{72}$	$-E_{45} + E_{18}$	$-E_{45} + E_{18}$
$-E_{47} + E_{38}$	$-E_{52} + E_{61}$	$-E_{34} + E_{87}$
$-E_{46} + E_{28}$	$E_{53} - E_{71}$	$-E_{24} + E_{86}$
$E_{41} - E_{58}$	$E_{41} - E_{58}$	$E_{36} - E_{27}$
$-E_{45} + E_{18}$	$-E_{63} + E_{72}$	$-E_{14} + E_{85}$
$E_{42} - E_{68}$	$E_{42} - E_{68}$	$-E_{35} + E_{17}$
$E_{43} - E_{78}$	$E_{43} - E_{78}$	$E_{25} - E_{16}$

Next we give the actions of the positive root vectors of heights 1, 5, 7, and 11 on the basis  $\beta' = \{v_0 - v_1, v_1 - v_2, v_3, v_4, \dots, v_{26}\}$  of  $\mathcal{J}_0$ , calculated using (\*) in 2.7.1. We shall write  $v'_1 = v_0 - v_1$  and  $v'_2 = v_1 - v_2$ , for brevity. The basis elements sent to 0 are omitted.



### Height 1

$$\begin{array}{llll}
e_{1000} : v_5 \mapsto v_4 & e_{0100} : v_3 \mapsto v_8 & e_{0010} : v'_1 \mapsto 2v_3 & e_{0001} : v'_1 \mapsto v_{15} \\
v_8 \mapsto -v_9 & v_4 \mapsto -v_7 & v'_2 \mapsto -v_3 & v'_2 \mapsto v_{15} \\
v_{13} \mapsto v_{12} & v_{17} \mapsto -v_{14} & v_7 \mapsto -v'_1 & v_3 \mapsto v_{26} \\
v_{16} \mapsto -v_{17} & v_{18} \mapsto v_{13} & v_{12} \mapsto -v_{25} & v_8 \mapsto v_{21} \\
v_{21} \mapsto v_{20} & v_{25} \mapsto -v_{22} & v_{13} \mapsto v_{24} & v_9 \mapsto -v_{20} \\
v_{24} \mapsto -v_{25} & v_{26} \mapsto v_{21} & v_{14} \mapsto -v_{19} & v_{10} \mapsto v_{23} \\
& & v_{15} \mapsto v_{26} & v_{11} \mapsto -v'_1 - v'_2 \\
& & v_{20} \mapsto -v_{17} & v_{19} \mapsto -v_6 \\
& & v_{21} \mapsto v_{16} & v_{22} \mapsto -v_7 \\
& & v_{22} \mapsto -v_{11} & v_{24} \mapsto v_5 \\
& & v_{23} \mapsto v_{18} & v_{25} \mapsto -v_4
\end{array}$$

### Height 5

$$\begin{array}{lll}
e_{1220} : v_4 \mapsto v_9 & e_{1121} : v'_1 \mapsto v_{17} & e_{0122} : v_9 \mapsto -v_6 \\
v_5 \mapsto -v_8 & v'_2 \mapsto v_{17} & v_{10} \mapsto v_5 \\
v_{15} \mapsto -v_{14} & v_5 \mapsto v_{26} & v_{11} \mapsto v_{16} \\
v_{18} \mapsto v_{11} & v_7 \mapsto v_{20} & v_{12} \mapsto -v_{15} \\
v_{23} \mapsto -v_{22} & v_8 \mapsto -v_{19} & v_{22} \mapsto -v_{21} \\
v_{26} \mapsto v_{19} & v_{10} \mapsto v_{25} & v_{25} \mapsto v_{26} \\
& v_{13} \mapsto -v'_1 - v'_2 & \\
& v_{21} \mapsto -v_6 & \\
& v_{22} \mapsto -v_9 & \\
& v_{23} \mapsto v_4 & \\
& v_{24} \mapsto -v_3 &
\end{array}$$

### Height 7

$$\begin{aligned} e_{1231} : v'_1 &\mapsto -v_{19} \\ v'_2 &\mapsto 2v_{19} \\ v_4 &\mapsto -v_{17} \\ v_5 &\mapsto v_{16} \\ v_7 &\mapsto -v_{14} \\ v_{10} &\mapsto v_{11} \\ v_{12} &\mapsto -v_9 \\ v_{13} &\mapsto v_8 \\ v_{15} &\mapsto -v_6 \\ v_{18} &\mapsto v_3 \\ v_{23} &\mapsto -v'_2 \end{aligned}$$

$$\begin{aligned} e_{1222} : v_3 &\mapsto v_6 \\ v_{10} &\mapsto -v_7 \\ v_{11} &\mapsto v_{14} \\ v_{18} &\mapsto -v_{15} \\ v_{24} &\mapsto v_{21} \\ v_{25} &\mapsto -v_{20} \end{aligned}$$

### Height 11

$$\begin{aligned} e_{2342} : v_5 &\mapsto v_6 \\ v_{10} &\mapsto -v_9 \\ v_{13} &\mapsto v_{14} \\ v_{18} &\mapsto -v_{17} \\ v_{23} &\mapsto v_{20} \\ v_{24} &\mapsto -v_{19} \end{aligned}$$

Finally we give below the maps  $R_5$ ,  $R_7$ ,  $R_{11}$ , and  $R_{13}$ , arising in 2.7.4. We also give the corresponding matrices with respect to the basis  $\beta_0 = \{w_1, w_2, \dots, w_{26}\}$  of  $\mathcal{J}_0$ , which we also denote by  $R_5$ ,  $R_7$ ,  $R_{11}$ , and  $R_{13}$ , respectively.

$$R_5 : v'_1 \mapsto -2v_{17}$$

$$v'_2 \mapsto v_{17}$$

$$v_3 \mapsto v_{14}$$

$$v_4 \mapsto v_{21}$$

$$v_5 \mapsto v_{26}$$

$$v_7 \mapsto -v_{16} - v_{20}$$

$$v_8 \mapsto -v_{19}$$

$$v_9 \mapsto -v_6$$

$$v_{10} \mapsto v_5$$

$$v_{11} \mapsto -v_{20}$$

$$v_{12} \mapsto v_3$$

$$v_{13} \mapsto v'_1$$

$$v_{18} \mapsto -v_7$$

$$v_{22} \mapsto -v_9 + v_{21}$$

$$v_{23} \mapsto v_4$$

$$v_{24} \mapsto v_3 + v_{15}$$

$$v_{25} \mapsto -v_8 - v_{26}$$

$$R_7 : v'_1 \mapsto -v_{19}$$

$$v'_2 \mapsto -v_{19}$$

$$v_4 \mapsto -v_{17}$$

$$v_5 \mapsto v_{20}$$

$$v_7 \mapsto -v_{14}$$

$$v_{10} \mapsto -v_{11}$$

$$v_{11} \mapsto -2v_{14}$$

$$v_{12} \mapsto 2v_{21}$$

$$v_{13} \mapsto v_8 + 3v_{26}$$

$$v_{15} \mapsto v_6$$

$$v_{18} \mapsto v_3 + 2v_{15}$$

$$v_{22} \mapsto -3v_{17}$$

$$v_{23} \mapsto v'_1 + v'_2$$

$$v_{24} \mapsto -v_9 + 2v_{21}$$

$$v_{25} \mapsto -2v_{16} - 2v_{20}$$

$$R_{11} : v_5 \mapsto v_6$$

$$v_{10} \mapsto -v_9 + 3v_{21}$$

$$v_{12} \mapsto -3v_{19}$$

$$v_{13} \mapsto 7v_{14}$$

$$v_{18} \mapsto -7v_{17}$$

$$v_{23} \mapsto 3v_{16} + 4v_{20}$$

$$v_{24} \mapsto -4v_{19}$$

$$v_{25} \mapsto -3v_6$$

$$R_{13} : v_{10} \mapsto -6v_{17}$$

$$v_{13} \mapsto 6v_6$$

$$v_{18} \mapsto -6v_{19}$$

$$v_{23} \mapsto 6v_{14}$$

The corresponding matrices are:

$$R_5 = -e_{17} - e_{29} + e_{3,11} - 2e_{4,13} + e_{4,14} - e_{5,15} - e_{6,15} - e_{6,16} - e_{7,18} + e_{8,17} + e_{8,18} \\ - e_{9,20} + e_{10,19} - e_{10,20} + e_{11,21} + e_{11,22} + e_{12,22} + e_{13,23} - e_{15,24} + e_{17,25} + e_{19,26}$$

$$R_7 = e_{1,12} - e_{2,13} - e_{2,14} - e_{3,15} - 2e_{3,16} - e_{4,17} - 3e_{4,18} - 2e_{5,20} + e_{6,19} - 2e_{6,20} \\ - e_{7,22} + 2e_{8,21} + 2e_{8,22} + e_{9,23} + 3e_{10,23} + e_{11,24} + 2e_{12,24} + e_{13,25} + e_{14,25} - e_{16,26}$$

$$R_{11} = e_{1,19} - 3e_{1,20} - 3e_{2,21} - 4e_{2,22} + 7e_{3,23} - 7e_{4,24} + 3e_{5,25} + 4e_{6,25} - e_{7,26} + 3e_{8,26}$$

$$R_{13} = 6(e_{1,23} - e_{2,24} + e_{3,25} - e_{4,26}) .$$

### 3.6 Appendix C

This section contains the matrices needed for type  $E_7$  (see 2.8). We first give the matrices  $\text{ade}_\alpha$ , where  $\alpha \in \{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_6\}$ . These are the matrices satisfying  $\text{ht}(\text{ade}_\alpha) = 1$ . Note the Dynkin diagram for  $E_7$  is given on p.vi.

$$\begin{aligned} \text{ade}_{(1)} = & e_{1,2} + e_{13,15} + e_{17,20} + e_{19,23} + e_{22,25} + e_{26,28} + e_{27,30} + e_{29,33} + e_{31,35} + e_{32,36} \\ & + e_{37,40} + e_{38,42} + e_{43,47} + e_{44,49} + e_{50,54} + e_{56,61} - 2e_{63,64} + e_{63,66} + e_{64,71} \\ & - e_{73,78} - e_{80,84} - e_{85,90} - e_{87,91} - e_{92,96} - e_{94,97} - e_{98,102} - e_{99,103} - e_{101,105} \\ & - e_{104,107} - e_{106,108} - e_{109,112} - e_{111,115} - e_{114,117} - e_{119,121} - e_{132,133} \end{aligned}$$

$$\begin{aligned} \text{ade}_{(2)} = & e_{4,5} + e_{6,8} + e_{7,10} + e_{9,14} + e_{27,31} + e_{30,35} + e_{32,37} + e_{34,39} + e_{36,40} + e_{38,43} \\ & + e_{41,46} + e_{42,47} + e_{44,50} + e_{48,53} + e_{49,54} + e_{55,60} - 2e_{62,65} + e_{62,67} + e_{65,72} \\ & - e_{74,79} - e_{80,85} - e_{81,86} - e_{84,90} - e_{87,92} - e_{88,93} - e_{91,96} - e_{94,98} - e_{95,100} \\ & - e_{97,102} - e_{99,104} - e_{103,107} - e_{120,125} - e_{124,127} - e_{126,128} - e_{129,130} \end{aligned}$$

$$\begin{aligned} \text{ade}_{(3)} = & e_{2,3} + e_{11,13} + e_{12,17} + e_{16,19} + e_{18,22} + e_{21,26} + e_{24,29} + e_{30,34} + e_{35,39} + e_{36,41} \\ & + e_{40,46} + e_{42,48} + e_{47,53} + e_{49,55} + e_{54,60} - e_{56,63} + e_{61,64} - 2e_{61,66} + e_{61,67} \\ & + e_{66,73} + e_{71,78} - e_{74,80} - e_{79,85} - e_{81,87} - e_{86,92} - e_{88,94} - e_{93,98} - e_{95,99} \\ & - e_{100,104} - e_{105,110} - e_{108,113} - e_{112,116} - e_{115,118} - e_{117,122} - e_{121,123} - e_{131,132} \end{aligned}$$

$$\begin{aligned} \text{ade}_{(4)} = & e_{3,4} + e_{8,11} + e_{10,12} + e_{14,16} + e_{22,27} + e_{25,30} + e_{26,32} + e_{28,36} + e_{29,38} + e_{33,42} \\ & + e_{39,45} + e_{46,52} - e_{50,56} + e_{53,59} - e_{54,61} - e_{55,62} + e_{60,65} + e_{60,66} - 2e_{60,67} \\ & + e_{60,68} + e_{67,74} + e_{72,79} + e_{73,80} - e_{75,81} + e_{78,84} - e_{82,88} - e_{89,95} - e_{92,101} \\ & - e_{96,105} - e_{98,106} - e_{102,108} - e_{104,109} - e_{107,112} - e_{118,120} - e_{122,124} - e_{123,126} \\ & - e_{130,131} \end{aligned}$$

$$\begin{aligned} \text{ade}_{(6)} = & e_{6,7} + e_{8,10} + e_{11,12} + e_{13,17} + e_{15,20} - e_{21,24} - e_{26,29} - e_{28,33} - e_{32,38} - e_{36,42} \\ & - e_{37,43} - e_{40,47} - e_{41,48} - e_{46,53} + e_{51,57} - e_{52,59} + e_{58,68} - 2e_{58,69} + e_{58,70} \\ & + e_{69,76} + e_{75,82} - e_{77,83} + e_{81,88} + e_{86,93} + e_{87,94} + e_{91,97} + e_{92,98} + e_{96,102} \\ & + e_{101,106} + e_{105,108} + e_{110,113} - e_{114,119} - e_{117,121} - e_{122,123} - e_{124,126} - e_{127,128}. \end{aligned}$$

Finally we give the matrices  $\text{ade}_\alpha$ , where  $\alpha \in \{\alpha_5, \alpha_7, \alpha_1 + \alpha_3, \alpha_2 + \alpha_4, \alpha_3 + \alpha_4\}$ , which are the matrices satisfying  $\text{ht}(\text{ade}_\alpha) = 2$ . The remaining root vectors can be generated using the set of structure constants for  $E_7$  given in [GS].

$$\begin{aligned}\text{ade}_{(5)} = & e_{4,6} + e_{5,8} + e_{12,18} + e_{16,21} + e_{17,22} + e_{19,26} + e_{20,25} + e_{23,28} - e_{38,44} - e_{42,49} \\ & - e_{43,50} + e_{45,51} - e_{47,54} - e_{48,55} + e_{52,58} - e_{53,60} + e_{59,67} - 2e_{59,68} + e_{59,69} \\ & + e_{68,75} + e_{74,81} - e_{76,82} + e_{79,86} + e_{80,87} - e_{83,89} + e_{84,91} + e_{85,92} + e_{90,96} \\ & - e_{106,111} - e_{108,115} - e_{109,114} - e_{112,117} - e_{113,118} - e_{116,122} - e_{126,129} - e_{128,130}\end{aligned}$$

$$\begin{aligned}\text{ade}_{(7)} = & -e_{7,9} - e_{10,14} - e_{12,16} - e_{17,19} - e_{18,21} - e_{20,23} - e_{22,26} - e_{25,28} - e_{27,32} - e_{30,36} \\ & - e_{31,37} - e_{34,41} - e_{35,40} - e_{39,46} - e_{45,52} - e_{51,58} + e_{57,69} - 2e_{57,70} + e_{70,77} \\ & + e_{76,83} + e_{82,89} + e_{88,95} + e_{93,100} + e_{94,99} + e_{97,103} + e_{98,104} + e_{102,107} + e_{106,109} \\ & + e_{108,112} + e_{111,114} + e_{113,116} + e_{115,117} + e_{118,122} + e_{120,124} + e_{125,127}\end{aligned}$$

$$\begin{aligned}\text{ade}_{(8)} = & e_{1,3} - e_{11,15} - e_{12,20} - e_{16,23} - e_{18,25} - e_{21,28} - e_{24,33} + e_{27,34} + e_{31,39} + e_{32,41} \\ & + e_{37,46} + e_{38,48} + e_{43,53} + e_{44,55} + e_{50,60} - e_{56,64} - e_{56,66} + e_{56,67} - e_{61,71} + e_{63,73} \\ & + e_{64,78} + e_{66,78} - e_{74,84} - e_{79,90} - e_{81,91} - e_{86,96} - e_{88,97} - e_{93,102} - e_{95,103} \\ & - e_{100,107} + e_{101,110} + e_{106,113} + e_{109,116} + e_{111,118} + e_{114,122} + e_{119,123} - e_{131,133}\end{aligned}$$

$$\begin{aligned}\text{ade}_{(9)} = & -e_{3,5} + e_{6,11} + e_{7,12} + e_{9,16} - e_{22,31} - e_{25,35} - e_{26,37} - e_{28,40} - e_{29,43} - e_{33,47} \\ & + e_{34,45} + e_{41,52} - e_{44,56} + e_{48,59} - e_{49,61} - e_{55,65} + e_{55,66} - e_{55,67} + e_{55,68} - e_{60,72} \\ & + e_{62,74} + e_{65,79} + e_{67,79} + e_{73,85} - e_{75,86} + e_{78,90} - e_{82,93} + e_{87,101} - e_{89,100} \\ & + e_{91,105} + e_{94,106} + e_{97,108} + e_{99,109} + e_{103,112} - e_{118,125} - e_{122,127} - e_{123,128} \\ & + e_{129,131}\end{aligned}$$

$$\begin{aligned}\text{ade}_{(10)} = & e_{2,4} - e_{8,13} - e_{10,17} - e_{14,19} + e_{18,27} + e_{21,32} + e_{24,38} - e_{25,34} - e_{28,41} - e_{33,48} \\ & + e_{35,45} + e_{40,52} + e_{47,59} - e_{49,62} - e_{50,63} + e_{54,64} + e_{54,65} - e_{54,66} - e_{54,67} + e_{54,68} \\ & - e_{60,73} + e_{61,74} + e_{66,80} + e_{67,80} + e_{71,84} + e_{72,85} - e_{75,87} - e_{82,94} + e_{86,101} \\ & - e_{89,99} + e_{93,106} - e_{96,110} + e_{100,109} - e_{102,113} - e_{107,116} + e_{115,120} + e_{117,124} \\ & + e_{121,126} - e_{130,132}.\end{aligned}$$

# Bibliography

- [B1] N. Bourbaki, *Algebra II, Chapters 4-7*, Springer-Verlag, Berlin, 1990.
- [B2] ———, *Groupes et Algebres de Lie, Chapitres 7 et 8*, Hermann, Paris, 1975.
- [B3] ———, *Groupes et Algebres de Lie, Chapitres 2 et 3*, Hermann, Paris, 1972.
- [BdS] A. Borel and J. de Siebenthal, *Les sous-groupes fermés de rang maximum des groupes de Lie clos*, Comment. Math. Helv. **23** (1949), 200-221.
- [Bo] A. Borel, *Linear Algebraic Groups, Second Enlarged Edition*, Springer-Verlag, New York, 1991.
- [BT] A. Borel and J. Tits, *Compléments à l'article 'Groupes réductifs'*, Inst. Hautes Etudes Sci. Publ. Math. **41** (1972), 253-276.
- [Bu] D.M. Burton, *Elementary Number Theory, Revised Printing*, Wm. C. Brown Publishers, Iowa, 1988.
- [C1] R.W. Carter, *Simple Groups of Lie Type*, Wiley-Interscience, London, 1972.
- [C2] ———, *Finite Groups of Lie Type: Conjugacy Classes and Complex Characters*, Wiley-Interscience, Chichester, 1985.
- [Cu] C.W. Curtis, *Chevalley Groups and Related Topics, Finite Simple Groups*, Academic Press, London (1971), 135-189.
- [Di] J. Dieudonné, *La Géométrie des Groupes Classiques, Troisième Édition*, Springer-Verlag, Berlin, 1971.

- [DM] F. Digne and J. Michel, *Representations of Finite Groups of Lie Type*, *LMS Student Texts* 21, Cambridge Uni. Press, Cambridge, 1991.
- [GS] P.B. Gilkey and G.M. Seitz, *Some representations of exceptional Lie algebras*, *Geom. Dedicata* **25** (1988), 407-416.
- [H1] J.E. Humphreys, *Introduction to Lie Algebras and Representation Theory*, Springer-Verlag, New York, 1972.
- [H2] ———, *Linear Algebraic Groups*, Springer-Verlag, New York, 1975.
- [H3] ———, *Conjugacy Classes in Semisimple Algebraic Groups*, *Mathematical Surveys and Monographs*, Vol. 43,, Amer. Math. Soc., Rhode Island, 1995.
- [Ha] M. Hazewinkel, *Formal Groups and Applications*, Academic Press, New York, 1978.
- [HT] T. Hawkes, *Lie Algebras*, Lecture Course Notes, Warwick, 1993.
- [J1] N. Jacobson, *Lie Algebras*, Dover Publications, New York, 1979.
- [J2] ———, *A note on three-dimensional simple Lie algebras*, *J. Math. Mech.* **7** (1958), 823-831.
- [J3] ———, *Exceptional Lie Algebras*, Marcel Dekker, New York, 1971.
- [J4] ———, *Basic Algebra II, Second Edition*, Freeman, San Francisco, 1989.
- [K] G. Karpilovsky, *Topics in Field Theory*, *North-Holland Mathematics Studies* 155, Elsevier Science Publishers B.V., Amsterdam, 1989.
- [L] S. Lang, *Algebra, Second Edition*, Addison-Wesley, California, 1984.
- [La] R. Lawther, *Jordan block sizes of unipotent elements in exceptional algebraic groups*, *Comm. Algebra* **23** (1995), 4125-4156.
- [LS] M.W. Liebeck and G.M. Seitz, *Reductive subgroups of exceptional algebraic groups*, *Mem. Amer. Math. Soc.* **580** (1996).
- [LT] R. Lawther and D.M. Testerman,  *$A_1$ -subgroups of exceptional algebraic groups*, *Warwick Preprints* **74** (1995).



- [R] R. Ree, *On some simple groups defined by C. Chevalley*, Trans. Amer. Math. Soc. **84** (1957), 392-400.
- [S] J.-P. Serre, *Algebraic Groups and Class Fields*, Springer-Verlag, New York, 1988.
- [Sc] R.D. Schafer, *An Introduction to Non-Associative Algebras*, Academic Press, New York, 1966.
- [Se1] G.B. Seligman, *On automorphisms of Lie algebras of classical type II*, Trans. Amer. Math. Soc. **94** (1960), 452-482.
- [Se2] ———, *On automorphisms of Lie algebras of classical type III*, Trans. Amer. Math. Soc. **97** (1960), 286-316.
- [Sp1] T.A. Springer, *A note on centralizers in semi-simple groups*, Indag. Math. **28** (1966), 75-77.
- [Sp2] ———, *Some arithmetical results on semi-simple Lie algebras*, Inst. Hautes Etudes Sci. Publ. Math. **30** (1966), 115-141.
- [Sp3] ———, *Linear Algebraic Groups*, Birkhäuser, Boston, 1981.
- [SS] T.A. Springer and R. Steinberg, *Conjugacy classes, Seminar on Algebraic Groups and Related Finite Groups, Lecture Notes in Math., vol. 131*, Springer-Verlag, Berlin (1970), 167-266.
- [SSz] J. Saxl and G.M. Seitz, *Subgroups of algebraic groups containing regular unipotent elements*, J. London Math. Soc. (2) **55** (1997), no.2, 370-386.
- [St] R. Steinberg, *Lectures on Chevalley Groups*, Yale Univ. Math. Dept., 1968.
- [Sz] G.M. Seitz, *Maximal subgroups of exceptional algebraic groups*, Mem. Amer. Math. Soc. **441** (1991).
- [T1] D.M. Testerman, *The construction of the maximal  $A_1$ 's in the exceptional algebraic groups*, Proc. Amer. Math. Soc. **116** (1992), 635-644.
- [T2] ———,  *$A_1$ -type overgroups of elements of order  $p$  in semisimple algebraic groups and the associated finite groups*, J. Algebra **177** (1995), 34-76.

- [T3] ———, *Irreducible subgroups of exceptional algebraic groups*, Mem. Amer. Math. Soc. **390** (1988).
- [Ti] J. Tits, *Classification of algebraic semisimple groups*, Proc. Symp. Pure Math. (A.M.S.) **9** (1966), 33-62.
- [W] H. Weyl, *The Classical Groups, 2nd edition*, Princeton Univ. Press, New Jersey, 1946.
- [Wi] E. Witt, *Zyklische körper und algebren der charackteristik  $p$  von grad  $p^n$ , struktur diskret bewerteter perfekter körper mit vollkommenem restklassenkörper der charackteristik  $p$* , J. für Math. **176** (1936), 126-140.
- [ZS] O. Zariski and P. Samuel, *Commutative Algebra, Volume II, GTM 29*, Springer-Verlag, New York, 1960.